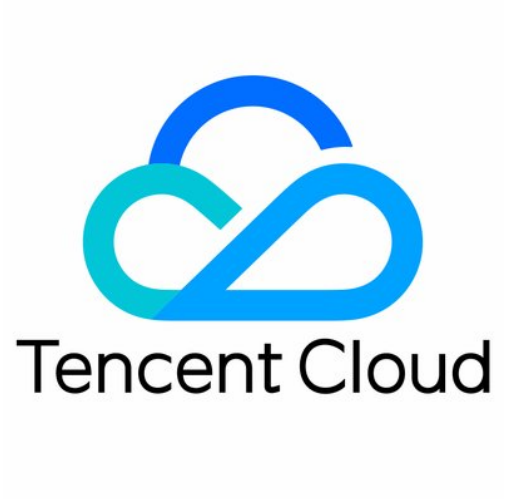
Anti-DDoS Advanced

Operation Guide

Product Documentation



Contents

Unblocking an IP

Operation Guide
Operation Overview

Last updated：2022-07-06 17:08:59

This document lists the references for common operations in Anti-DDoS Advanced.

Reference

- Viewing security protection overview
- Use Limits

Protection Configuration

DDoS protection

- Protection Level and Cleansing Threshold
- Protocol blocking
- Watermark protection
- Attribute Filtering
- AI protection
- IP blocklist/allowlist
- Port Filtering
- Regional Blocking
- IP and Port Rate Limiting
- Connection Attack Protection

CC protection

- Protection level and cleansing threshold
- Targeted protection
- CC frequency control
- Regional Blocking
- IP Blocklist/Allowlist

Business Connection

- Port connection
- Domain name connection
- Configuring session persistence
- Configuring health check

Instance Management

- Viewing instance information
- Setting instance alias and tag
- Modifying elastic protection bandwidth

Scheduling and Unblocking

Configuring intelligent scheduling

Operation Log

Viewing operation log

Blocking Operations

Unblocking an IP

Protection Overview

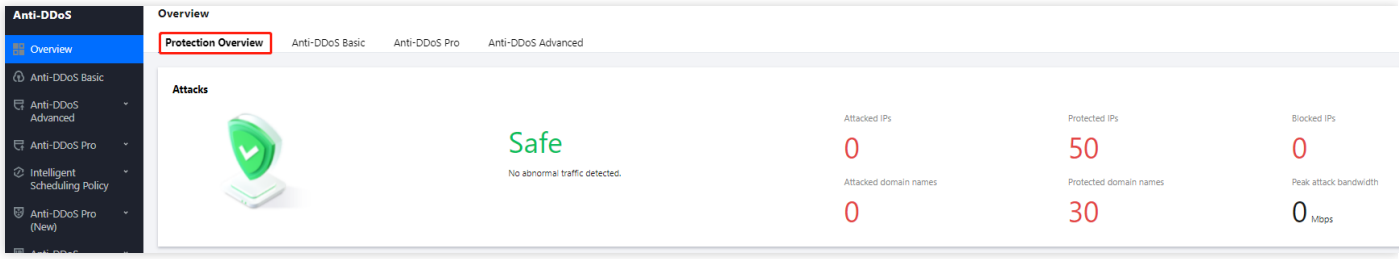
Last updated：2022-06-10 14:10:15

Protection Overview

The protection overview page of the Anti-DDoS console shows you complete, real-time indicators for basic protection, Anti-DDoS Pro, and Anti-DDoS Advanced applications, including the protection status and DDoS attack events, which can be used for analysis and source tracing.

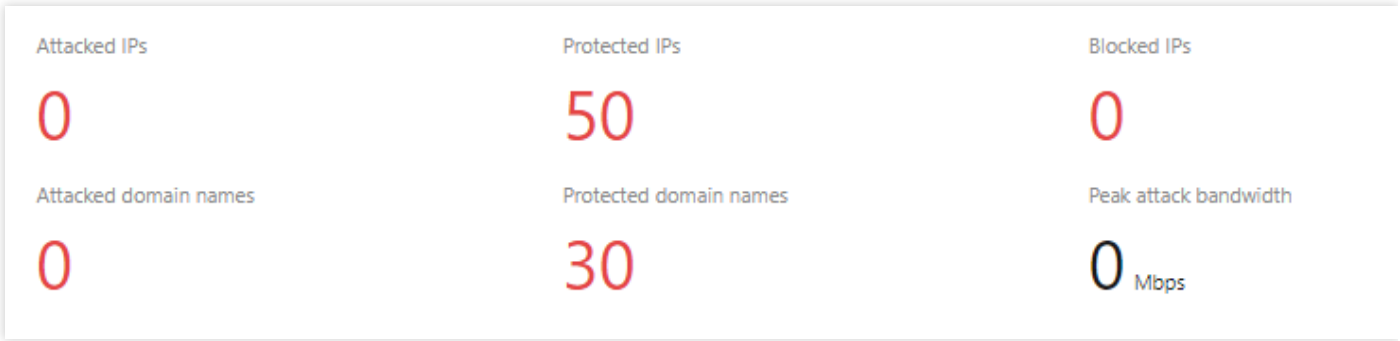
Viewing attack statistics

1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.



2. In the "Attacks" module, you can view the application security status, the latest attack and the attack type. To obtain higher protection, you can click **Upgrade Protection**.

3. This module also displays the details of the following data.



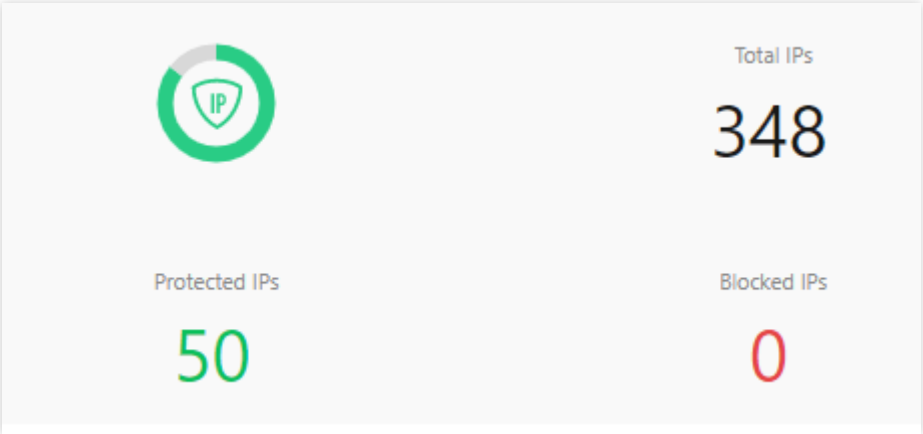
Field description:

- Attacked IPs: The total number of attacked application IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.

- Protected IPs: The total number of protected application IPs of Anti-DDoS Pro and Anti-DDoS Advanced.
- Blocked IPs: The total number of blocked IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.
- Attacked domain names: The total number of domain names of attacked Anti-DDoS Advanced instances and ports.
- Protected domain names: The number of domain names connected to Anti-DDoS Advanced instances.
- Peak attack bandwidth: The maximum attack bandwidth of the current attack events.

Viewing defense statistics

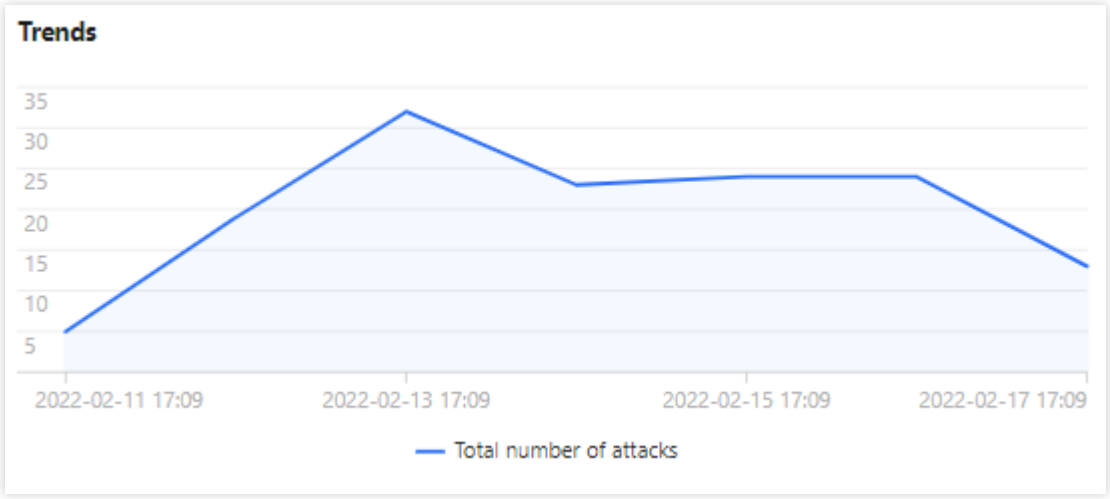
1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.
2. In the "Defense" module, you can easily see the application IP security status.



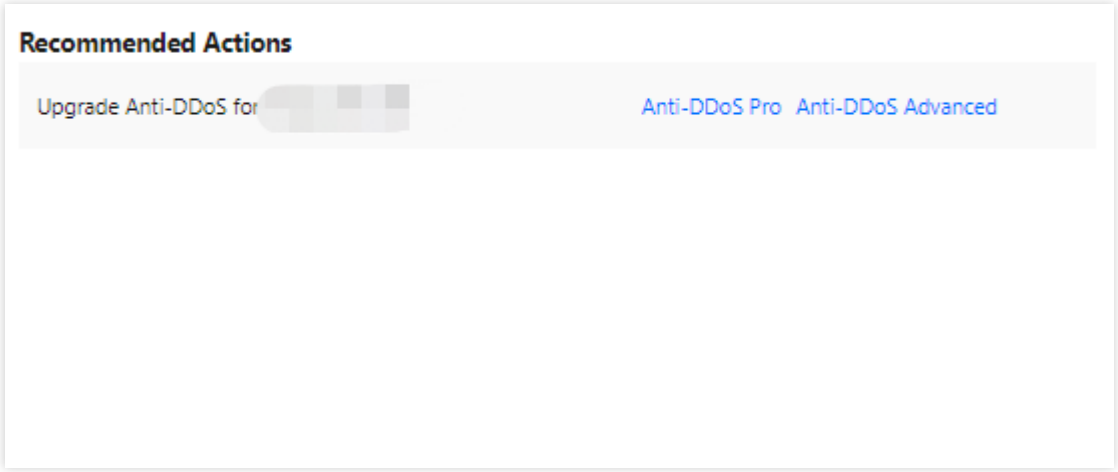
Field description:

- Total IPs: The total number of application IPs, including IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.
- Protected IPs: The total number of protected application IPs of Anti-DDoS Pro and Anti-DDoS Advanced.
- Blocked IPs: The total number of blocked IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.

3. This module also displays the total number of attacks on your applications, giving you a picture of the distribution of attacks.

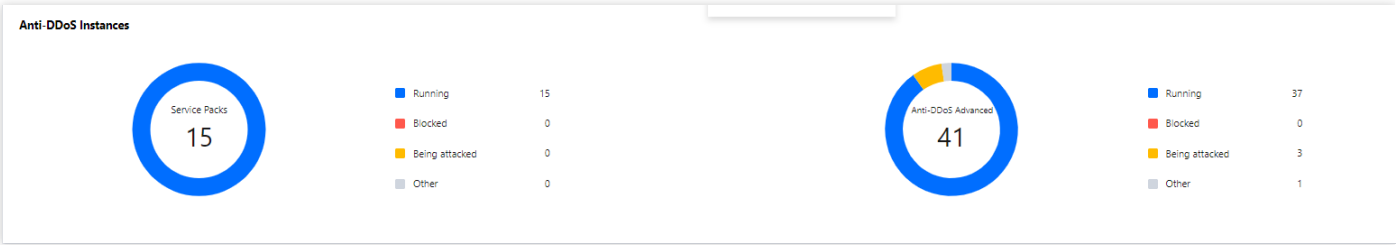


4. Meanwhile, this module provides recommended actions for the attacked IPs connected to basic protection, allowing you to quickly upgrade your Anti-DDoS service.



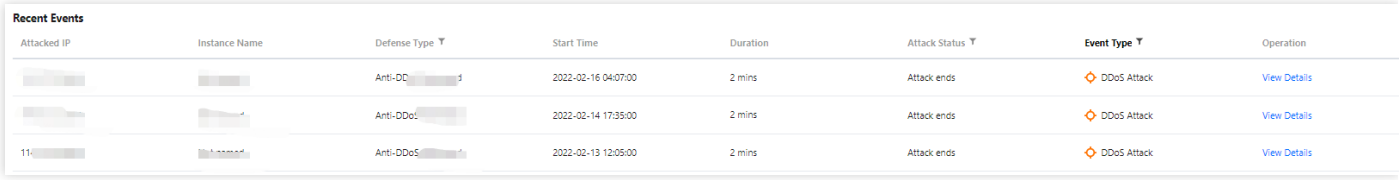
Viewing Anti-DDoS Advanced instance statistics

1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.
2. The "Anti-DDoS Instances" module visualizes the Anti-DDoS instance status data, providing an easy and complete way to know the distribution of insecure applications.

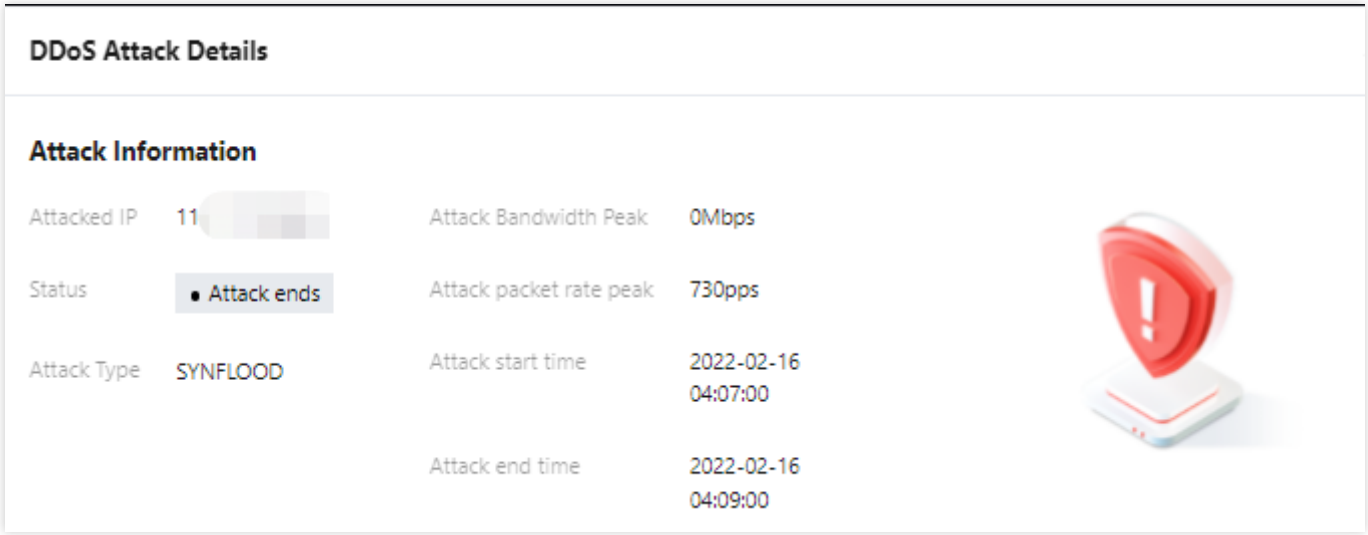


Viewing recent events

1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.
2. The "Recent Events" module shows you all the recent attack events. For attack analysis and source tracing, click **View Details** to enter the event details page.

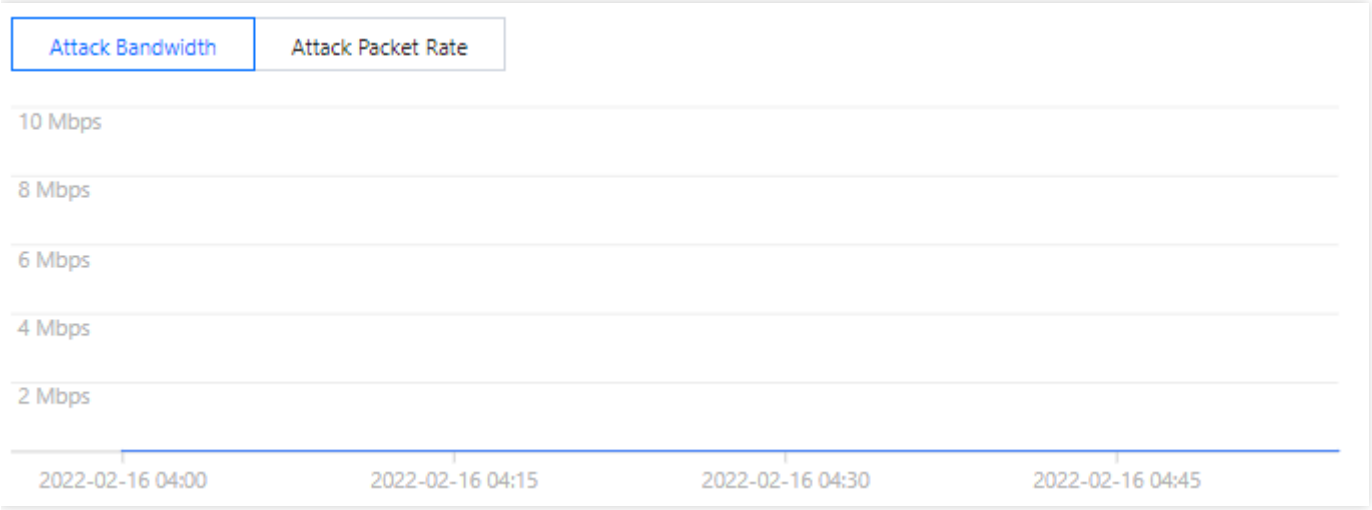


3. In the "Attack Information" module of the event details page, you can view the detailed attack information for the selected period, including the attacked IP, status, attack type (which is sampled data), peak attack bandwidth and attack packet rate, and attack start and end time.



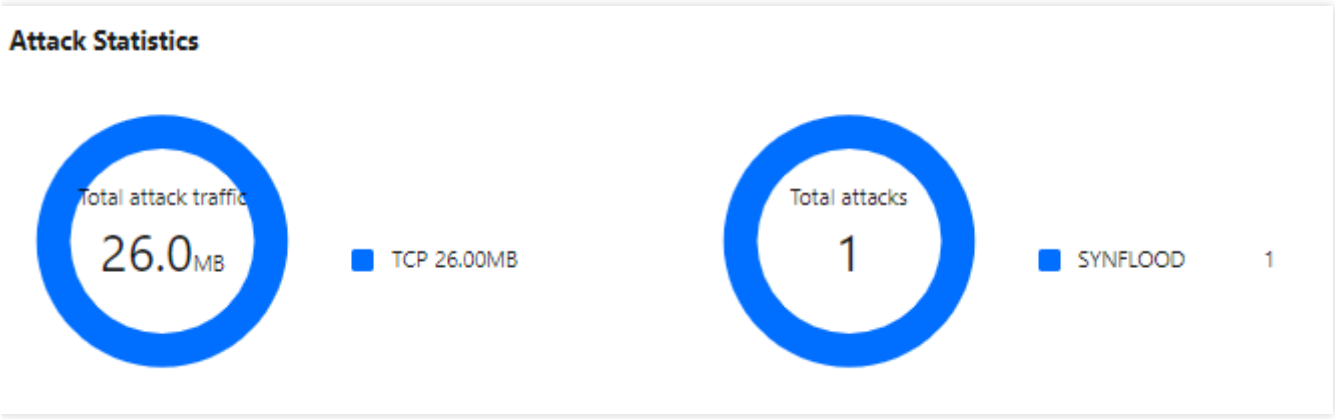
4. In the "Attack Trend" module of the event details page, you can view the trend of attack bandwidth and attack packet rate and easily find the peak spikes.

> Note：
> This module provides complete, real-time data in the attack period.



5. In the "Attack Statistics" module of the event details page, you can view how attacks distribute over different attack traffic protocols and attack types.

> Note：
> This module provides sampled data in the attack period.

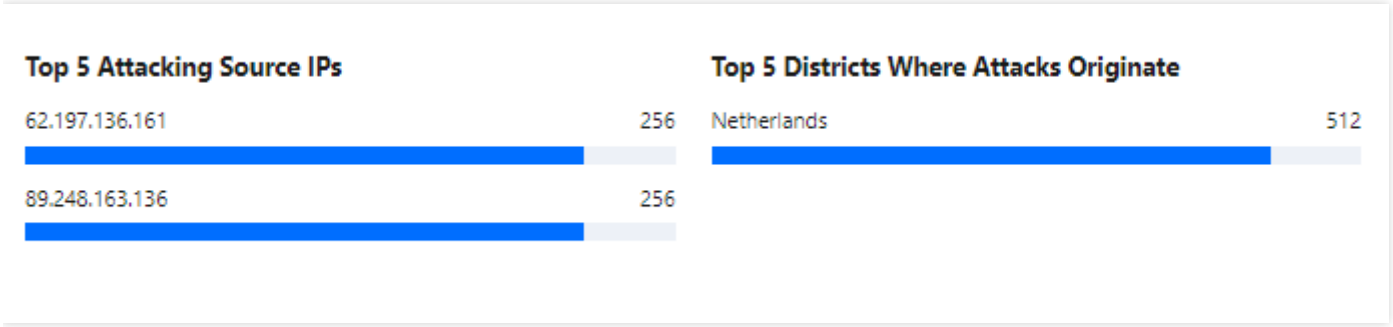


Field description:

- Attack traffic protocol distribution: It displays how attacks on the selected Anti-DDoS Advanced instance distribute over different attack traffic protocols within the queried period.
- Attack type distribution: It displays how attacks on the selected Anti-DDoS Advanced instance distribute over different attack types within the queried period.

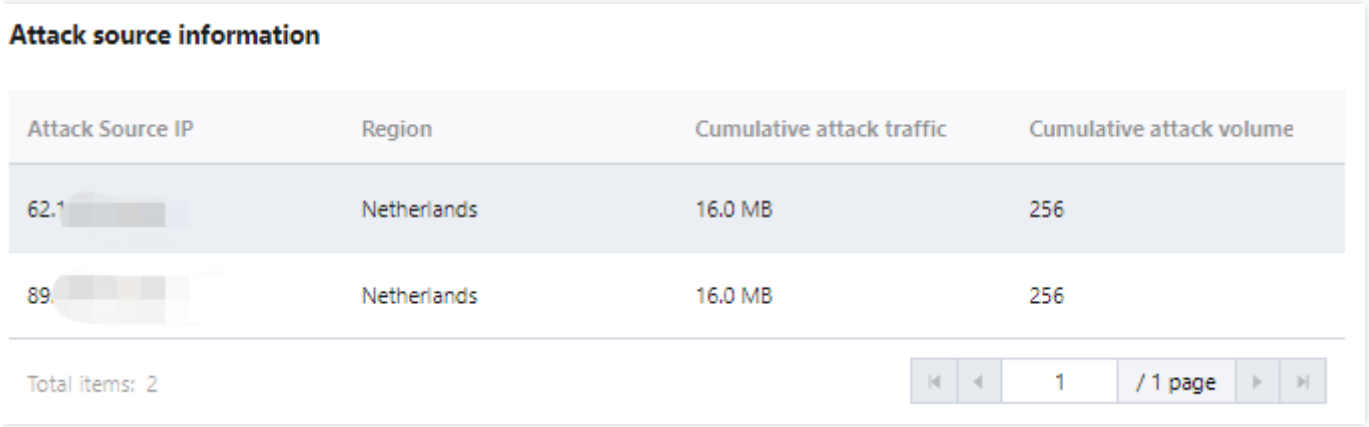
6. The "Top 5" modules of the event details page displays the top 5 attacker IP addresses and the top 5 attacker regions, which is helpful to precise protection configuration.

Note：
This module provides sampled data in the attack period.



7. In the "Attacker Information" module of the event details page, you can view the sampled data of the attack period, including the attacker IP, region, total attack traffic, and total attack packets.

Note：
This module provides sampled data in the attack period.

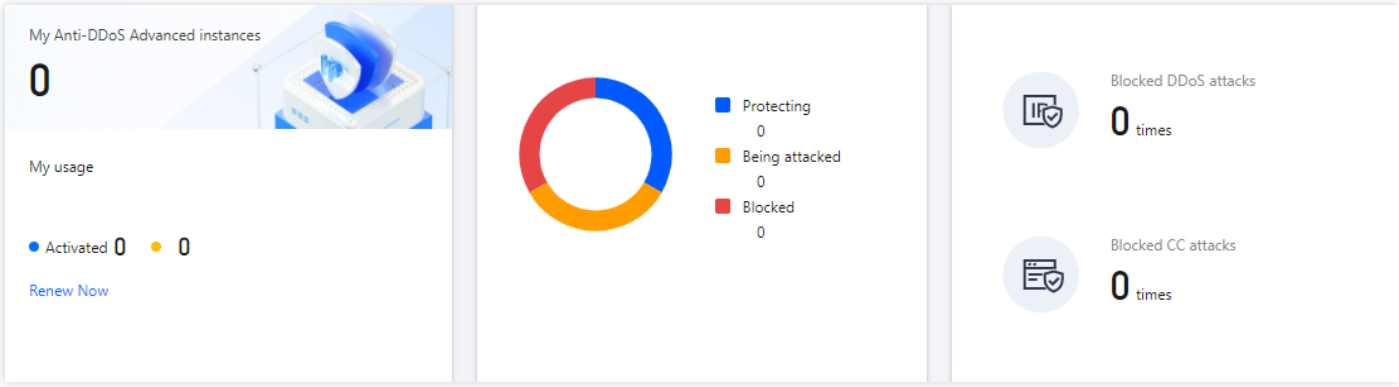


Anti-DDoS Advanced Overview

After an IP address is bound to an Anti-DDoS Advanced instance, when you receive a DDoS attack alarm message or notice any issue with your business, you need to view the attack details in the console, including the attack traffic and current protection effect. Enough information is critical for you to take measures to keep your business running smoothly.

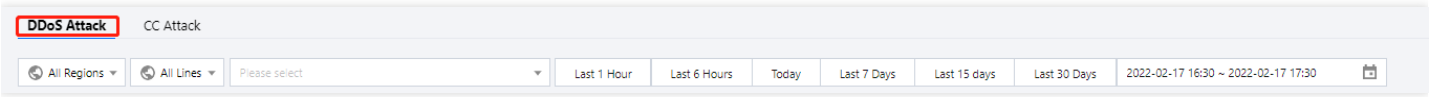
Viewing DDoS protection details

1. Log in to the new Anti-DDoS console, select **Overview** on the left sidebar and then open the **Anti-DDoS Advanced** tab.

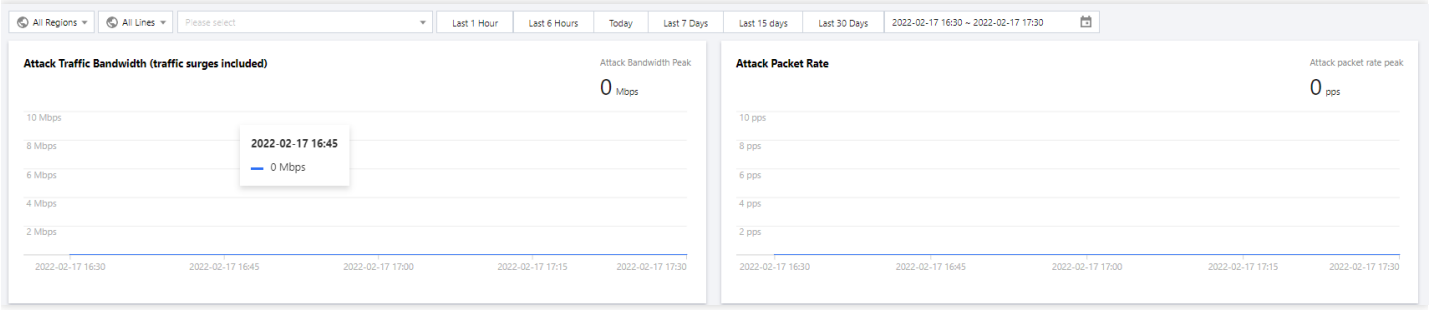


2. On the **DDoS Attack** tab, select a query period, target region, and an instance to check whether the instance has been attacked. The complete attack data is displayed by default.

> Note：
> You can query attack traffic and DDoS attack events in the past 180 days.

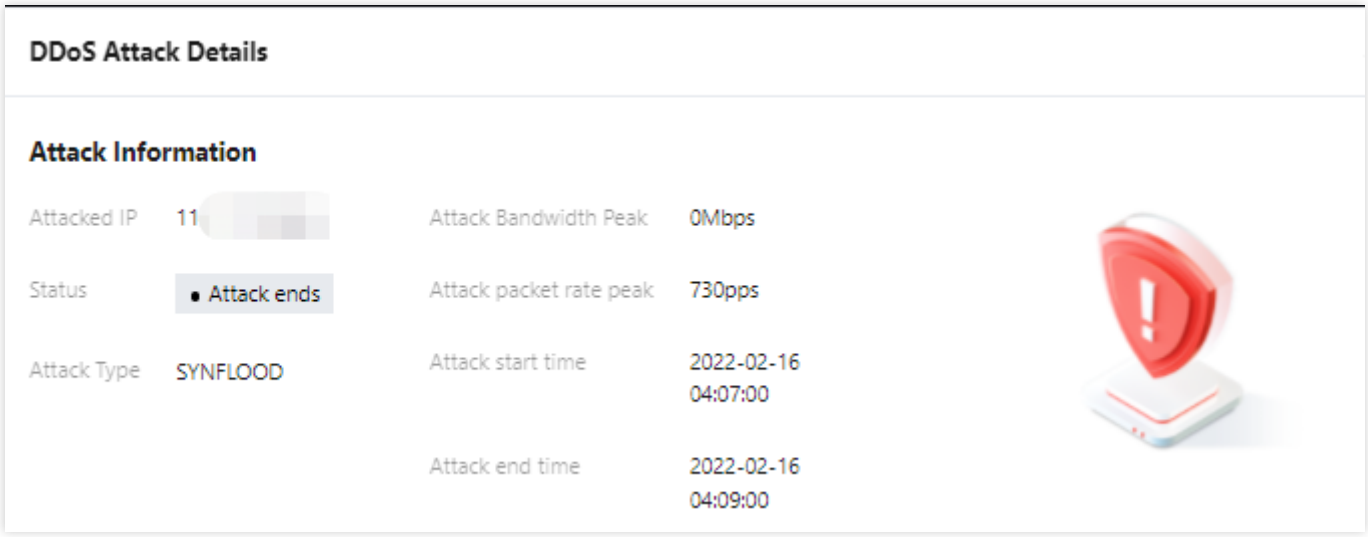


2. View the information of attacks suffered by the selected Anti-DDoS Advanced instance within the queried period, such as the trends of attack traffic bandwidth and attack packet rate.

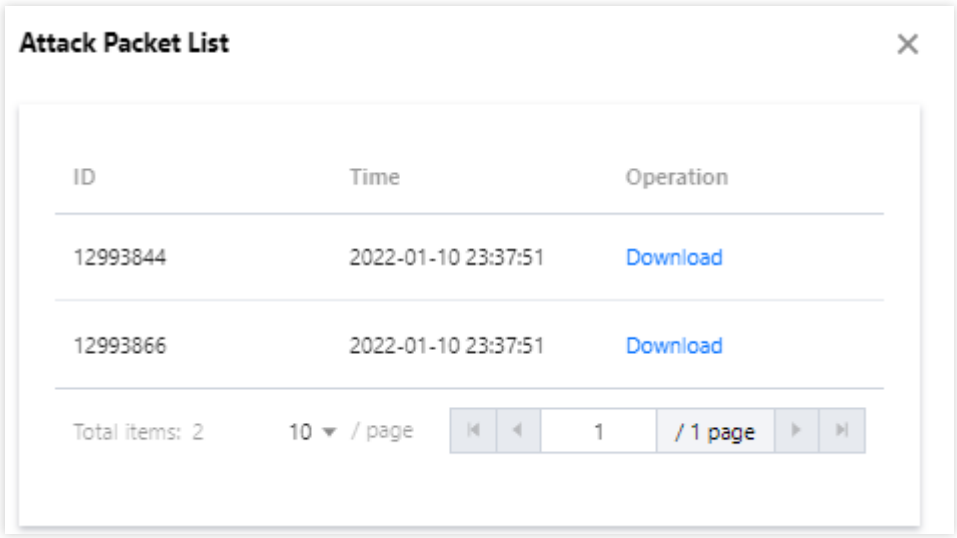


3. You can view the recent DDoS attacks in the **Recent Events** section. To view details of an event, you can click **View Details**. To view sampled attack data within a period, click **Packet Download**.

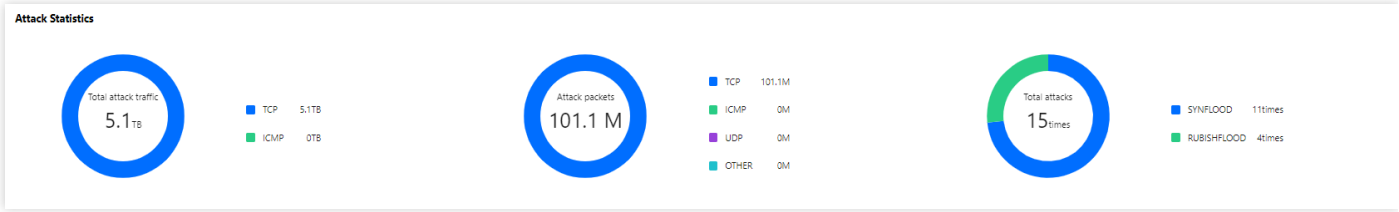
- View Details: You can view information including attacker IP, attack source region, generated attack traffic, and attack packet size, providing support for your source analysis and tracing.



- Packet Download: The sampled attack packet data can be downloaded to help customize a protection plan.



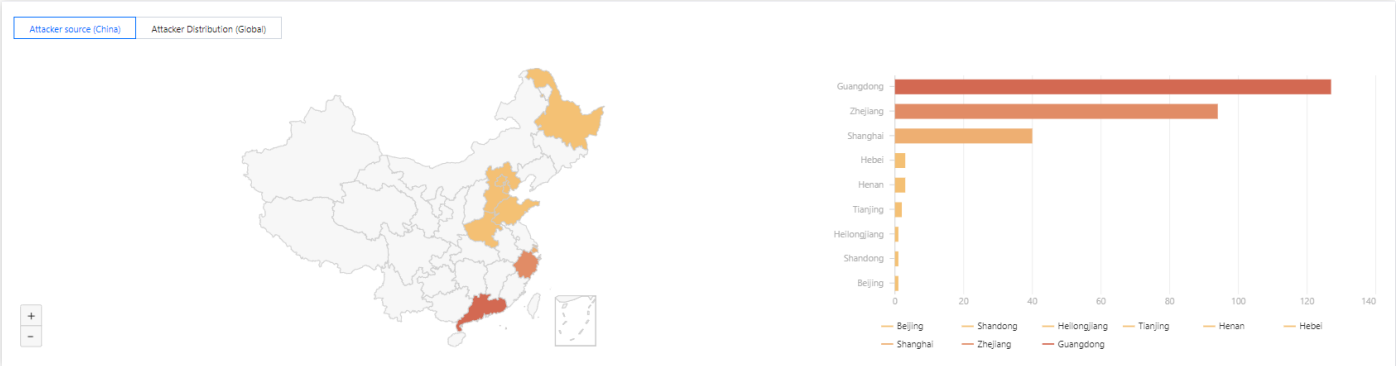
4. In the **Attack Statistics** section, you can view how the attacks distribute across different attack traffic protocols, attack packet protocols, and attack types.



Field description:

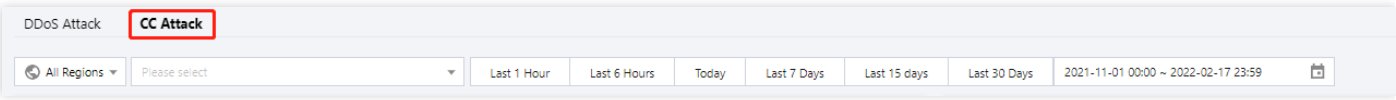
- Attack traffic protocol distribution: It displays how attacks on the selected Anti-DDoS Advanced instance distribute over different attack traffic protocols within the queried period.
- Attack packet protocol distribution: It displays how the attacks suffered by the selected Anti-DDoS Advanced instance distribute across different attack packet protocols within the queried period.
- Attack type distribution: It displays how attacks on the selected Anti-DDoS Advanced instance distribute over different attack types within the queried period.

5. In the attack source section, you can view the distribution of DDoS attack sources in and outside the Chinese mainland within the queried period, so that you can take further protective measures.

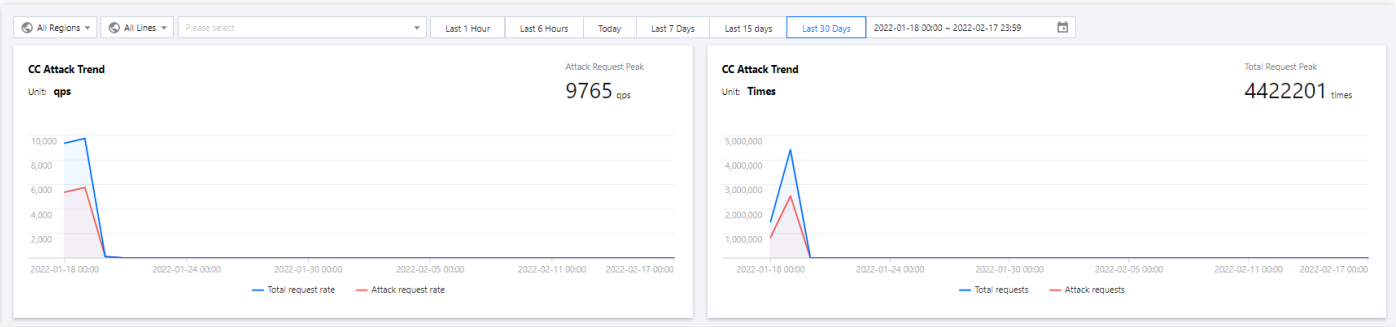


Viewing CC protection details

1. On the **CC Protection** tab, select a query period, target region, and an instance to check whether the instance has been attacked.



2. You can select **Today** to view the following data to identify the impact of attacks on your business.



Field description:

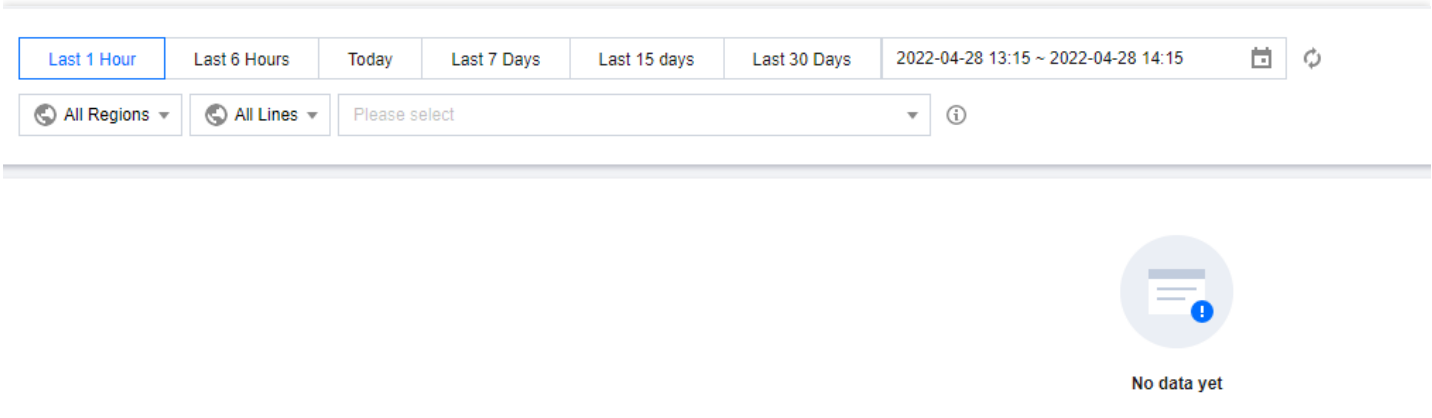
- Total request rate: The rate of total traffic (in QPS).
- Attack request rate: The rate of attack traffic (in QPS).
- Total requests: The total number of requests received.
- Attack requests: The number of attack requests received.

3. You can view recent CC attacks in the **Recent Events** section. Click **View Details** on the right of an event to display the attack start and end time, attacked domain name, attacked URI, total request peak, attack request peak, and attacker IP. You can also check the attack information, attack trends, and detailed CC records.

Viewing User Traffic Details

1. Log in to the new Anti-DDoS console. Select **Anti-DDoS Advanced** > **Application Traffic** on the left sidebar.
2. Select a query period, target region, and an instance to check whether the instance has been attacked. The complete DDoS attack data is displayed by default.

> Note：
> You can query traffic usage and DDoS attack events in the past 180 days.



3. You can view the trends of inbound/outbound traffic, bandwidth and packet rate, as well as the number of active connections and new connections within the selected time period. The maximum bandwidth, connections and QPS can also be checked.

- Active connections: The number of TCP connections that are already established and currently active.
- New connections: The number of TCP connections that are newly established per second for communication between the client and the instance.

Use Limits

Last updated：2023-05-09 16:59:58

Scenario

We recommended that you use Anti-DDoS Advanced to protect business IP addresses or domain names for website (layer-7) and non-website (layer-4) businesses in and outside Tencent Cloud.

Capability

By default, one Anti-DDoS Advanced instance supports a total of 60 forwarding rules for layer-4 access and layer-7 access. An Anti-DDoS Advanced instance supports 500 forwarding rules at most. For non-website (layer-4) protocols, each rule supports 20 source IP addresses or domain names. For website (layer-7) protocols, each rule supports 16 source IP addresses or domain names.

> Note：
> The total number of forwarding rules is the sum of forwarding rules for TCP/UDP and HTTP/HTTPS, and the maximum total number can be up to 500. For TCP and UDP, if the same forwarding port number is used, two different forwarding rules need to be configured.

Blacklist/Whitelist

- For DDoS protection, up to 100 IP addresses can be added to the blacklist and the whitelist in total.
- A URL allowlist is not supported.

Available Regions

At present, Anti-DDoS Advanced is available both in and outside Chinese Mainland. Specifically, it is supported in the following regions outside Chinese Mainland: Hong Kong (China), Taiwan (China), Singapore, Seoul, Tokyo, Virginia, Silicon Valley, and Frankfurt.

Protection Configuration
DDoS protection
Protection Level and Cleansing Threshold

Last updated：2022-04-01 09:42:59

This document introduces the use cases of different protection levels and the actions Anti-DDoS Advanced takes to defend against DDoS attacks. You can follow this guide to set the DDoS protection levels in the console.

Use Cases

Anti-DDoS Advanced provides three available protection levels for you to adjust protection policies against different DDoS attacks. The details are as follows:

Protection Level	Protection Action	Description
Loose	• Filters SYN and ACK data packets with explicit attack attributes. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications. • Filters UDP data packets with explicit attack attributes.	• This cleansing policy is loose and only defends against explicit attack packets. • We recommend choosing this protection level when normal requests are blocked. Complex attack packets may pass through the security system.
Medium	• Filters SYN and ACK data packets with explicit attack attributes. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications. • Filters UDP data packets with explicit attack attributes. • Filters common UDP-based attack packets. • Actively verifies the source IPs of some access attempts.	• This cleansing policy is suitable for most businesses and capable of defending against common attacks. • The level Medium is chosen by default.

Strict	• Filters SYN and ACK data packets with explicit attack attributes. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications. • Filters UDP data packets with explicit attack attributes. • Filters common UDP-based attack packets. • Actively verifies the source IPs of some access attempts. • Filters ICMP attack packets. • Filters common UDP attack data packets. • Strictly checks UDP data packets.	This cleansing policy is strict. We recommend choosing this level when attack packets pass through the security system on Normal mode.

Note：

- If you need to use UDP in your business, please contact sales to customize an ideal policy for not letting the level Strict affect normal business process.
- The level Medium is chosen by default in each Anti-DDoS Advanced instance, and you can adjust the protection level as needed. Also, you can set the cleansing threshold, so that the traffic exceeding the set value can be automatically cleansed.

Prerequisites

You have successfully purchased an Anti-DDoS Advanced instance and set the protected target.

Directions

1. Log in to the DDoS console and click **Anti-DDoS Advanced (New)** -> **Configurations** on the left sidebar.
2. Select an Anti-DDoS Advanced ID or port from the left list, e.g., `212.64.xx.xx bgpip-000002jt` or `119.28.xx.xx bgpip-000002ju` -> `tcp:8000` .
3. Choose a protection level and set the cleansing threshold in the **DDoS Protection Level** section.

Configuration Parameters

- **Protection Level**
  For each Anti-DDoS Advanced instance with the protection enabled, the level Medium is chosen by default and you can adjust the protection level as needed.
- **Cleansing Threshold**
  - It refers to the threshold to trigger cleansing. If the traffic is below the threshold, the cleansing action will not be taken even if attacks are detected.
  - For each Anti-DDoS Advanced instance with the protection enabled, the cleansing threshold has a default value, and you can set the cleansing threshold as needed. The system will learn the change patterns of business traffic to generate a baseline.

> Note：
> If you have a clear concept about the threshold, set it as needed. Otherwise please leave it to the default value. Anti-DDoS will automatically learn through AI algorithms and generate the default threshold for you.

Protocol Blocking

Last updated：2023-04-28 16:48:50

Anti-DDoS supports blocking the source traffic accessing Anti-DDoS instances based on specified protocols, such as ICMP, TCP, UDP, and other protocols. After the configuration is completed, all matched access requests will be directly blocked. Due to the connectionless feature of UDP protocol (unlike TCP, which requires a three-way handshake process), it has natural security vulnerabilities. If you do not have UDP businesses, we recommend blocking the UDP protocol.

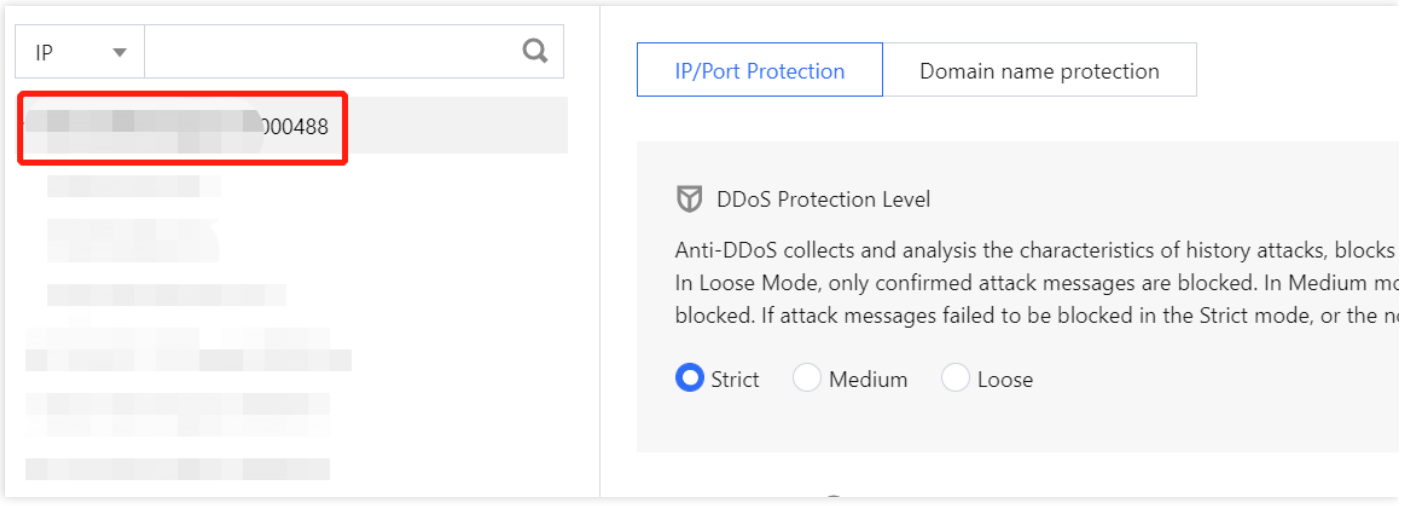
Prerequisites

- You have purchased an Anti-DDoS Advanced instance and set the target to protect.

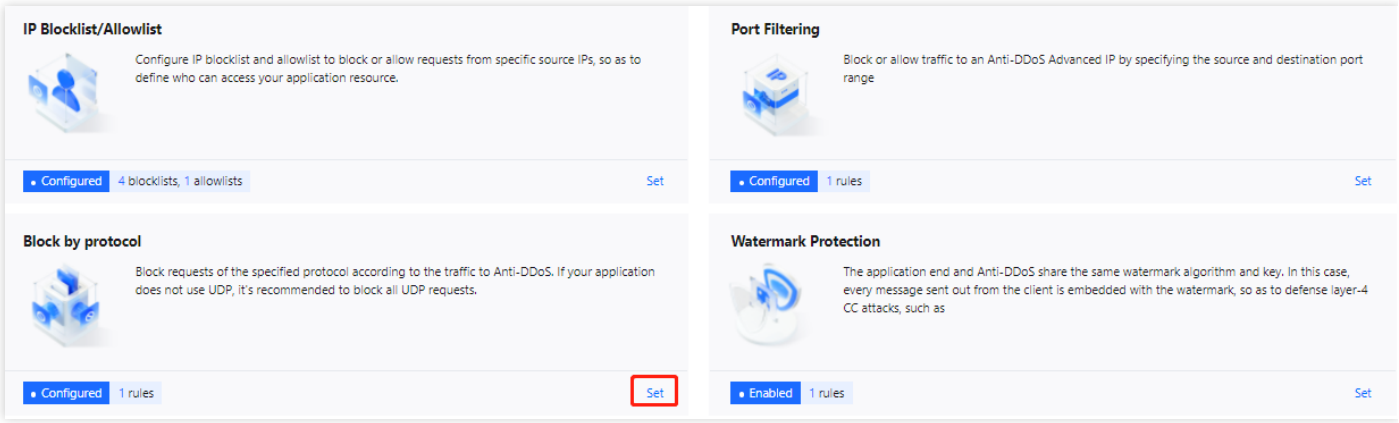
Directions

1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **DDoS Protection** tab.

2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".



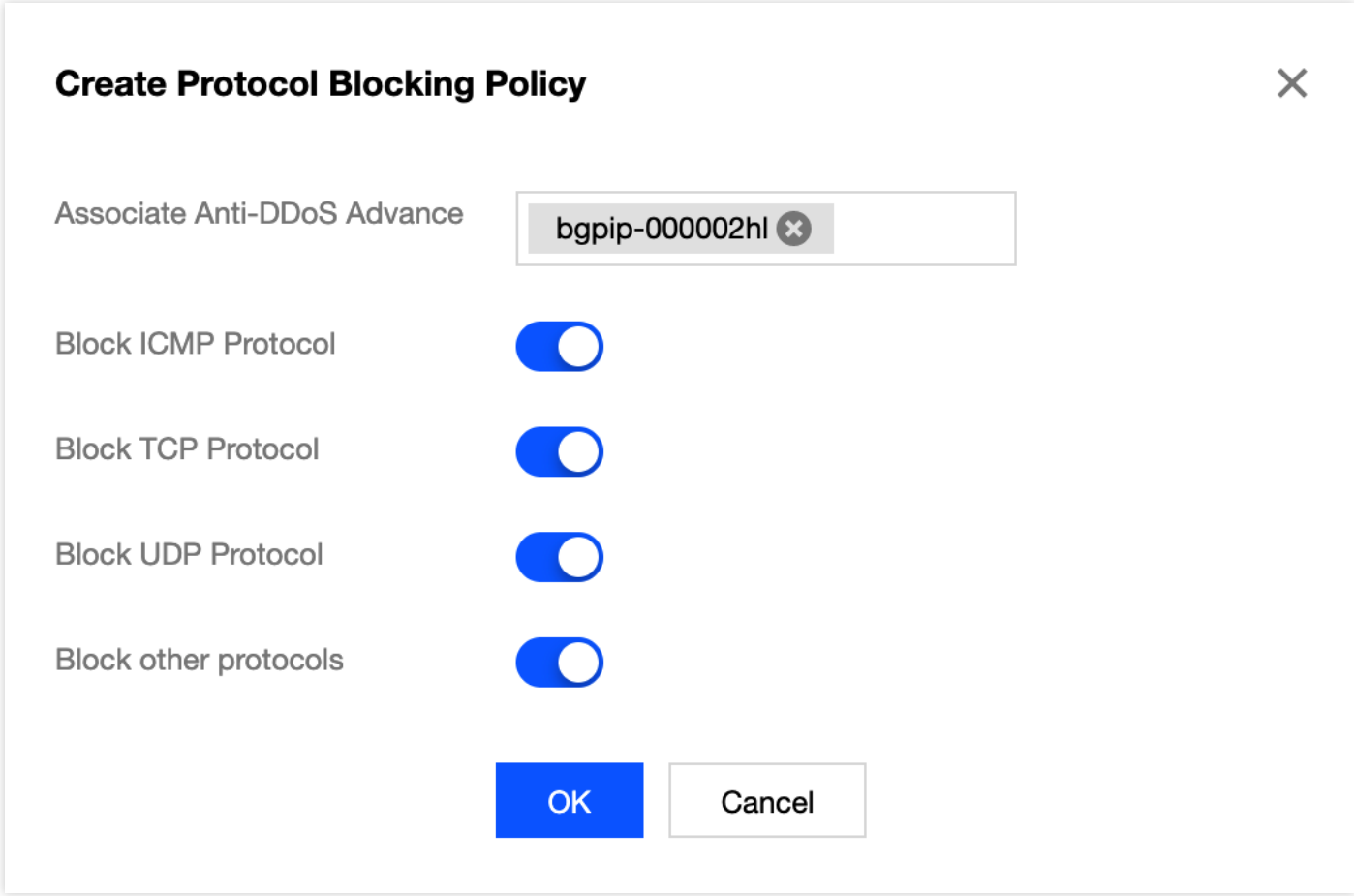
3. Click **Set** in the "Protocol blocking" section.



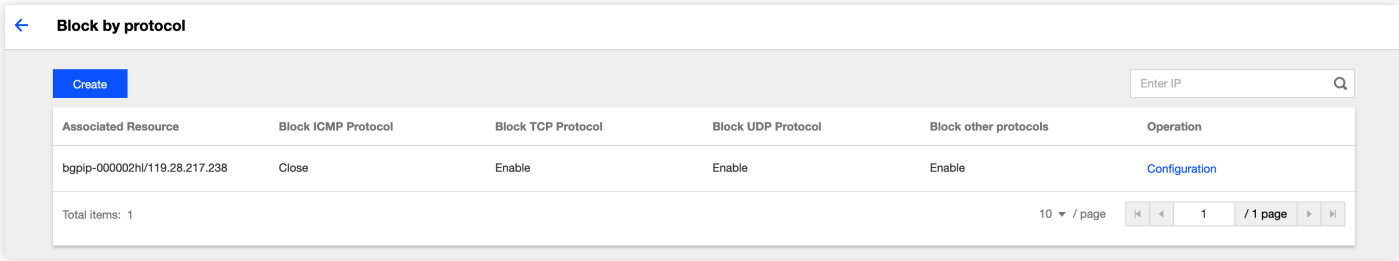
4. Click **Create**.

> Note：
> The **Create** button appears only when you use this feature for the first time.

5. In the pop-up window, click the button on the right of a protocol, and click **Confirm**.



6. After the rule is created, it is added to the list. You can click **Configuration** on the right of the rule to modify it.



Watermark Protection

Last updated：2022-03-11 12:30:54

Anti-DDoS supports watermark protection for the messages sent by the application end. Within the range of the UDP and TCP message ports configured, the application end and Anti-DDoS share the same watermark algorithm and key. After the configuration is completed, every message sent from the client will be embedded with the watermark while attack messages will not, so that the attack messages can be identified and discarded. Watermark protection can effectively and comprehensively defend against layer-4 CC attacks, such as analog business packet attacks and replay attacks.

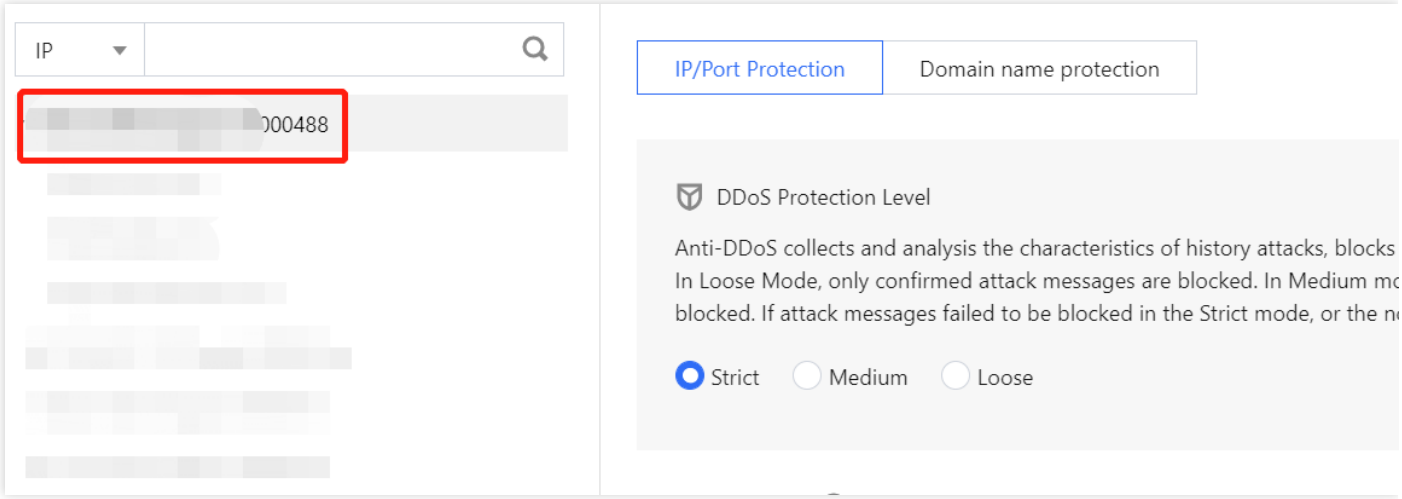
Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

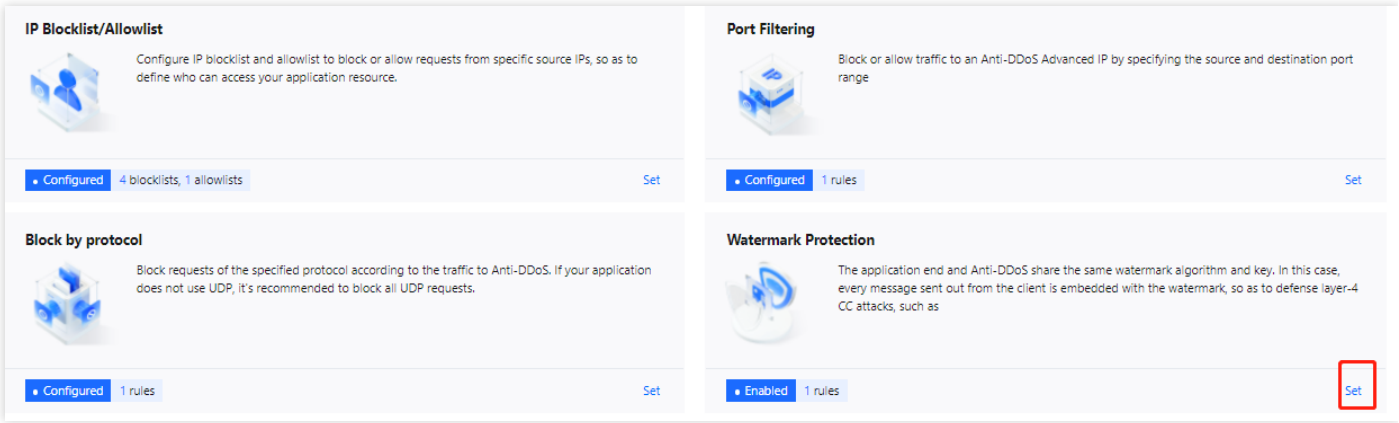
> Note：
> This feature is a paid service. Please contact us for activation.

Directions

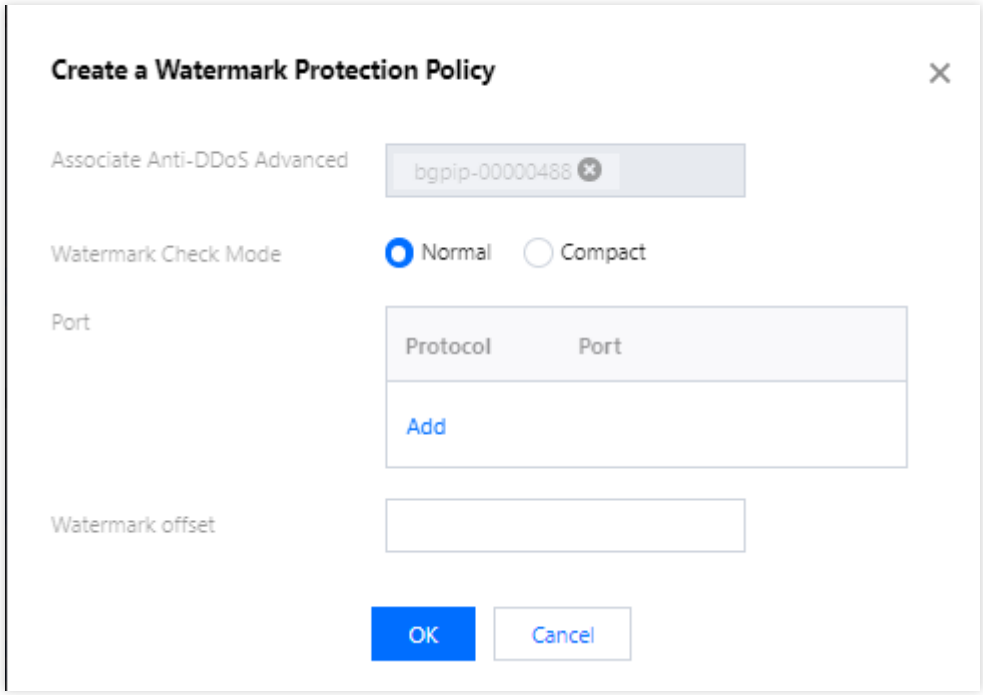
1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **DDoS Protection** tab.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".



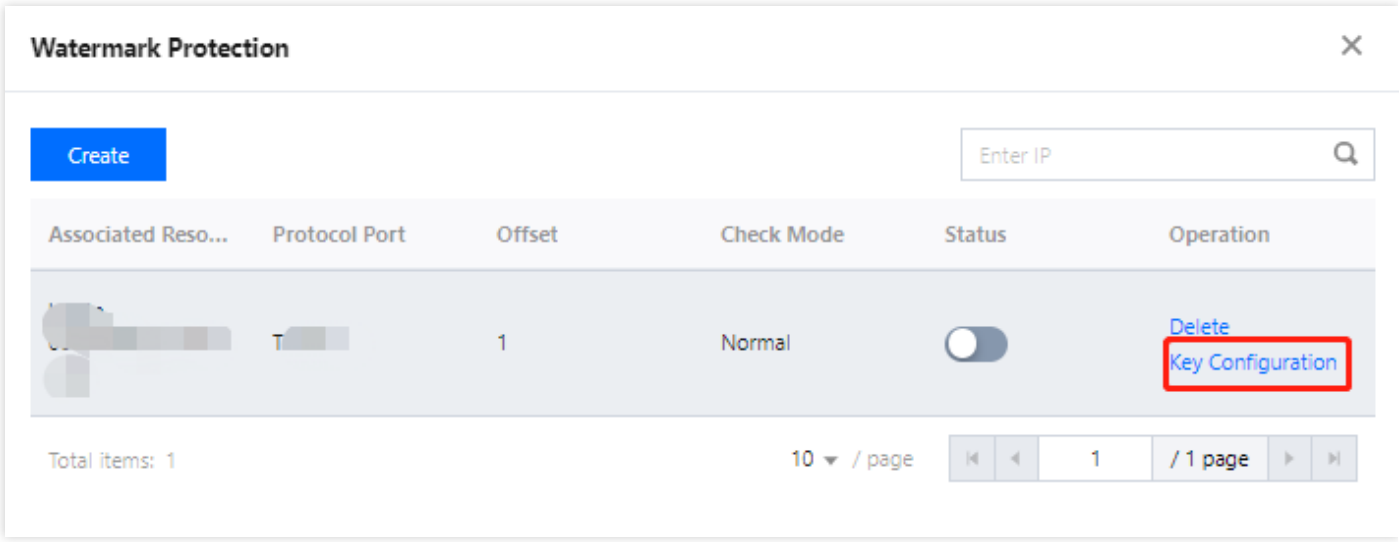
3. Click **Set** in the **Watermark Protection** section.



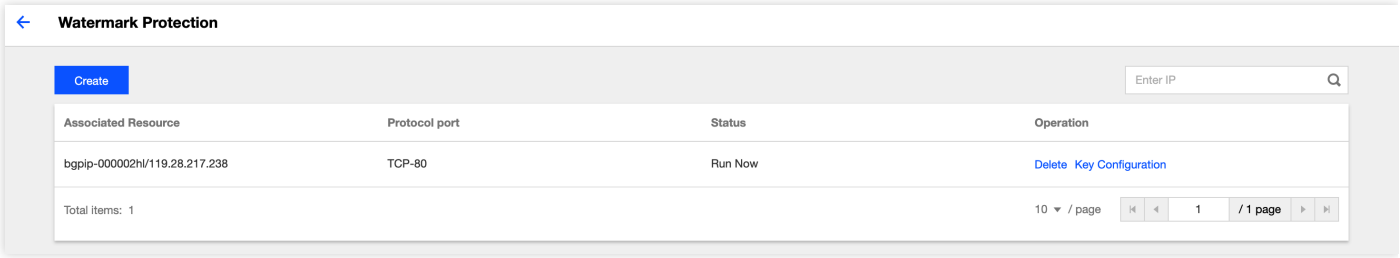
4. Click **Create**.
5. In the pop-up window, fill in the configuration fields and click **OK**.



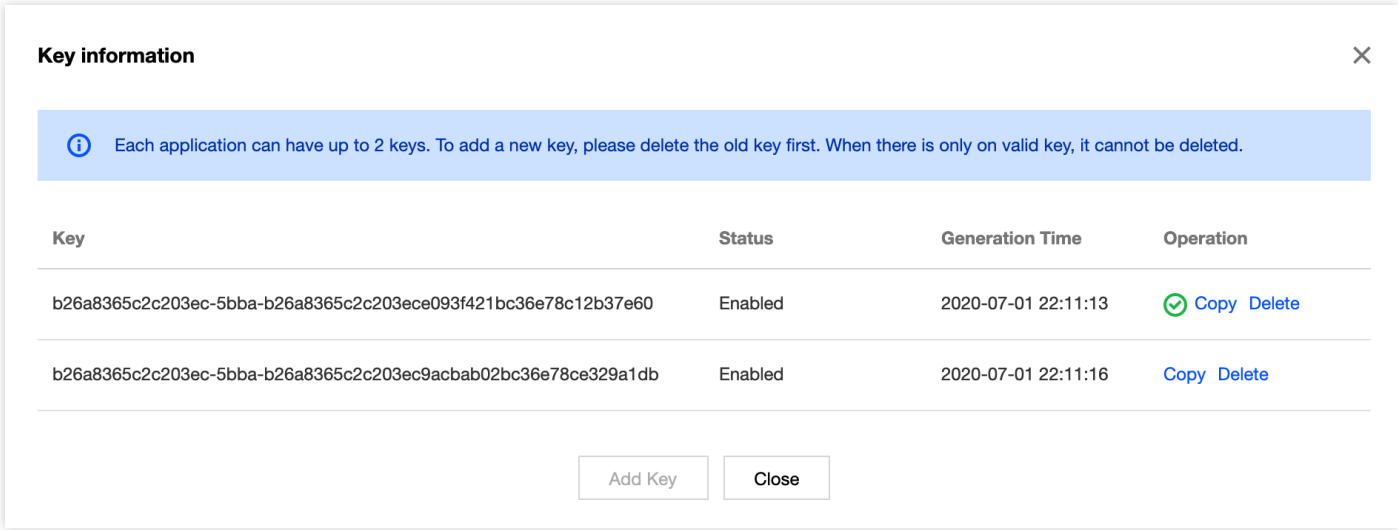
6. After the rule is created, it is added to the list. You can click **Key Configuration** to view and configure a key.



7. You can view and copy the key.



8. You can also add or delete a key on the key configuration page. A key can be deleted if you have another key. Up to two watermark keys can be created.



Feature Filtering

Last updated：2022-03-11 12:28:20

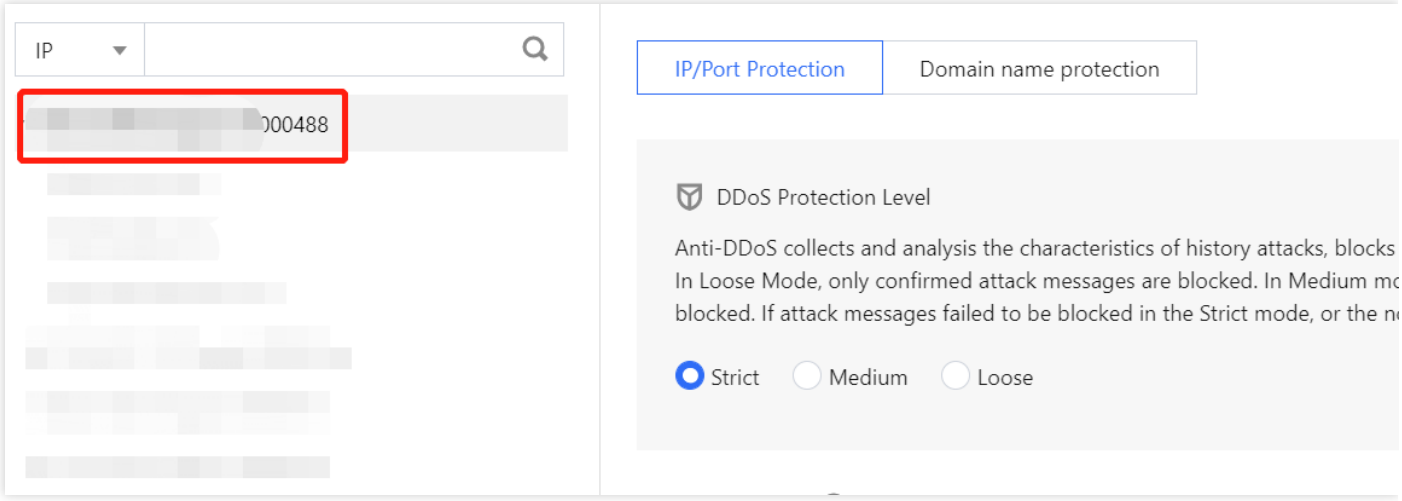
Anti-DDoS supports configuring custom blocking policies against specific IP, TCP, UDP message header or payload. After enabling feature filtering, you can combine the matching conditions of the source port, destination port, message length, IP message header or payload, and set the protection action to continue protection, allow/block/discard matched requests, block the IP for 15 minutes, or discard the request and then block the IP for 15 minutes, etc. With feature filtering, you can configure accurate protection policies against business message features or attack message features.

Prerequisites

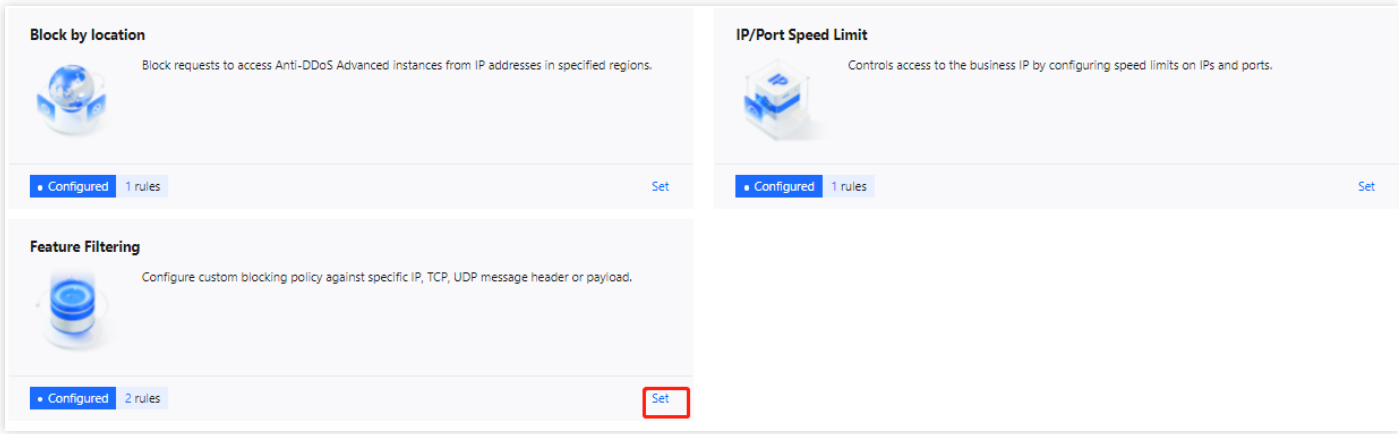
You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

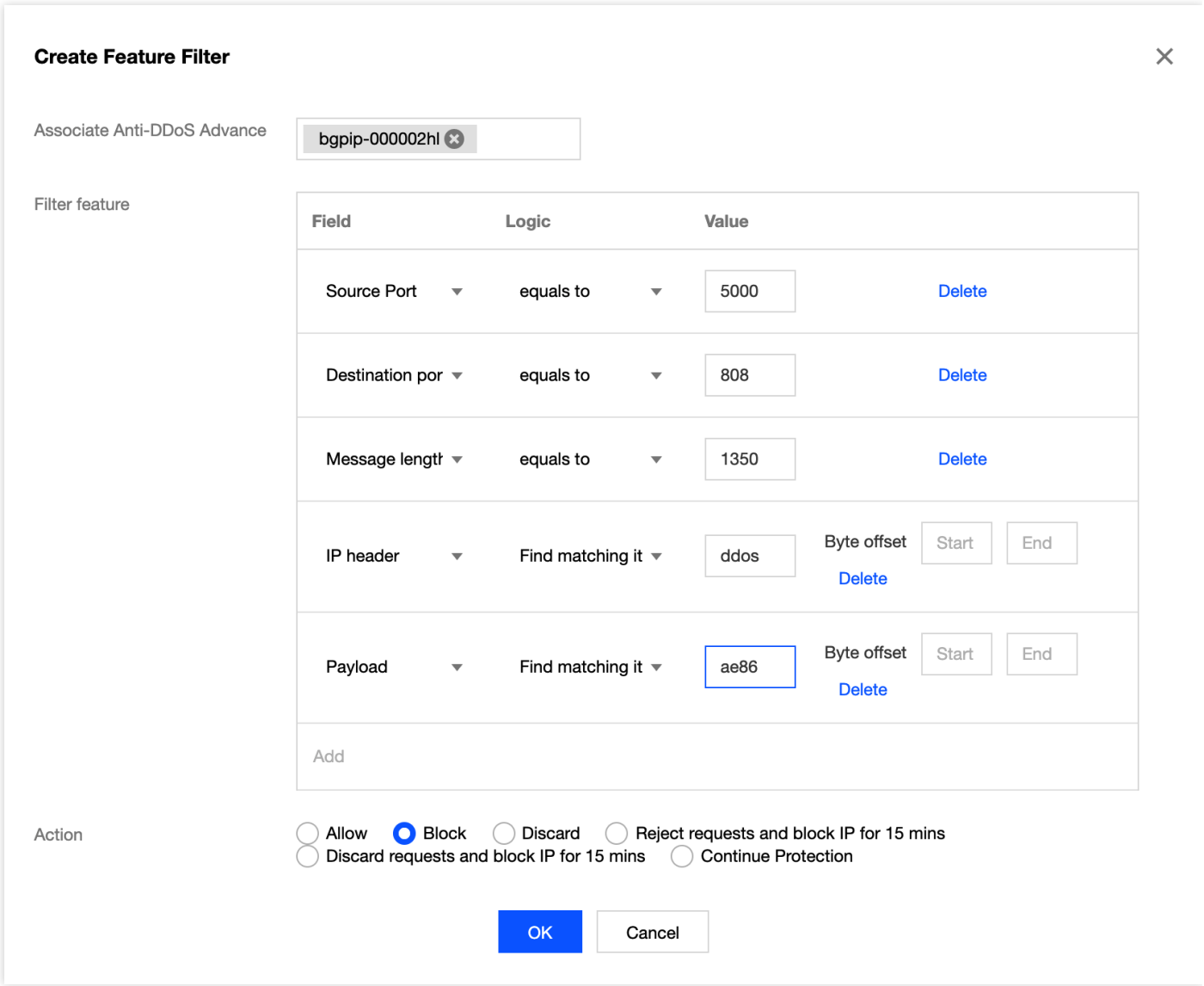
1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **DDoS Protection** tab.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".



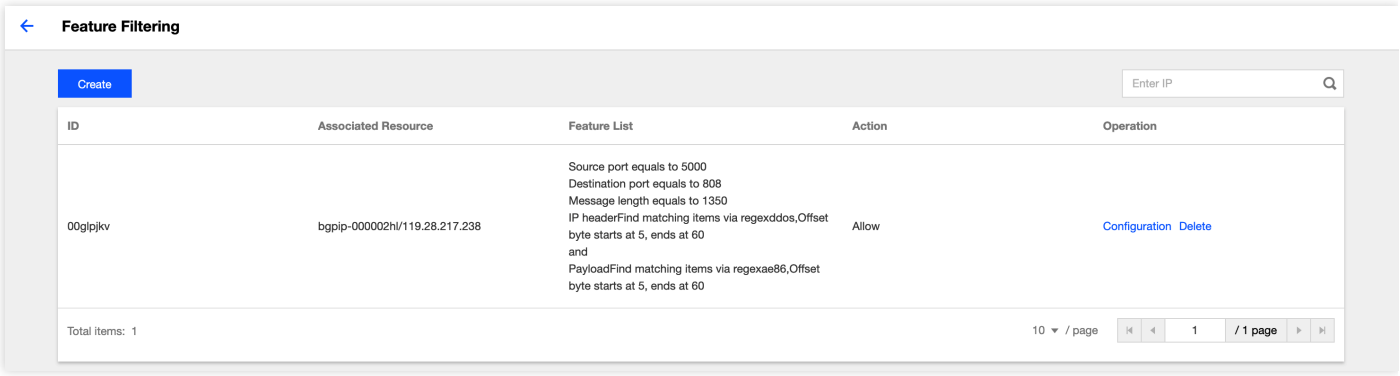
3. Click **Set** in the **Port Filtering** section to enter the port filtering page.



4. Click **Create**.
5. In the pop-up window, fill in the configuration fields, and click **OK**.



6. After the rule is created, it is added to the list. You can click **Configuration** on the right of the rule to modify it.



AI Protection

Last updated：2022-03-11 12:28:20

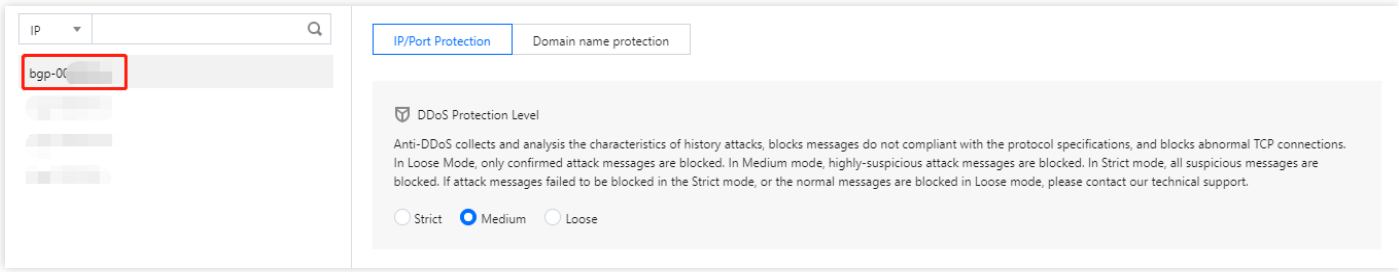
Anti-DDoS allows you to enable AI protection for powerful defense effect. With AI protection enabled, Anti-DDoS will learn connection baselines and traffic features using algorithms, auto-tune its cleansing policies, and detect and block 4-layer CC attacks.

Prerequisites

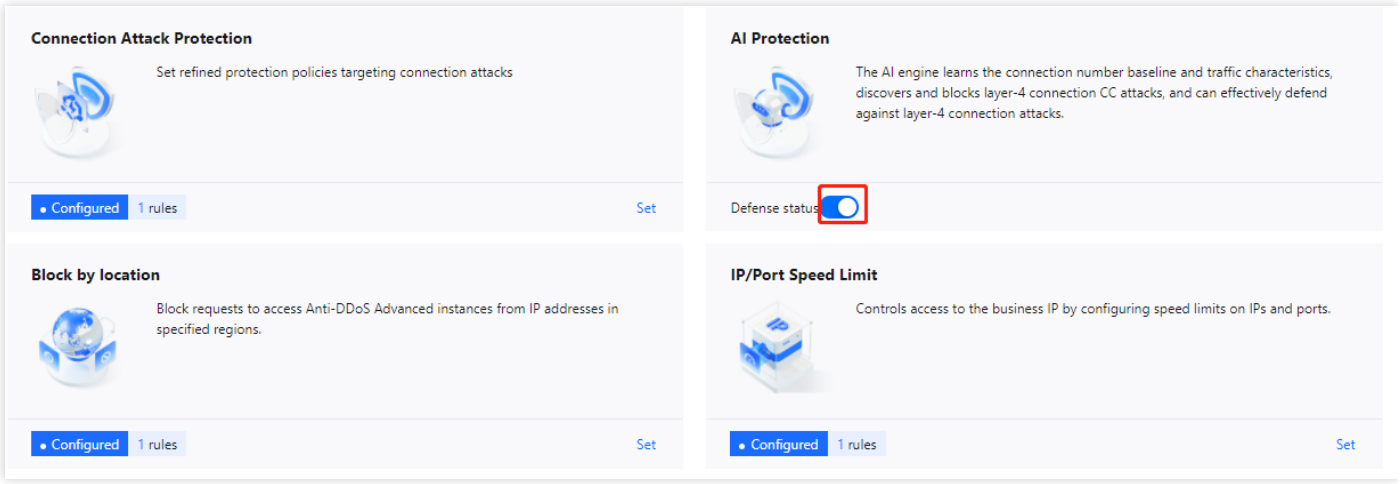
You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **DDoS Protection** tab.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".



3. Click in the **AI Protection** section to enable the setting.



IP Blocklist/Allowlist

Last updated：2023-04-28 16:48:50

Anti-DDoS supports configuring IP blocklist and allowlist to block or allow source IPs accessing the Anti-DDoS services, restricting the users accessing your business resources. If the accessing traffic exceeds the cleansing threshold, the allowed IPs will be allowed to access resources without being filtered by any protection policy; while the access requests from the blocked IPs will be directly denied.

Prerequisites

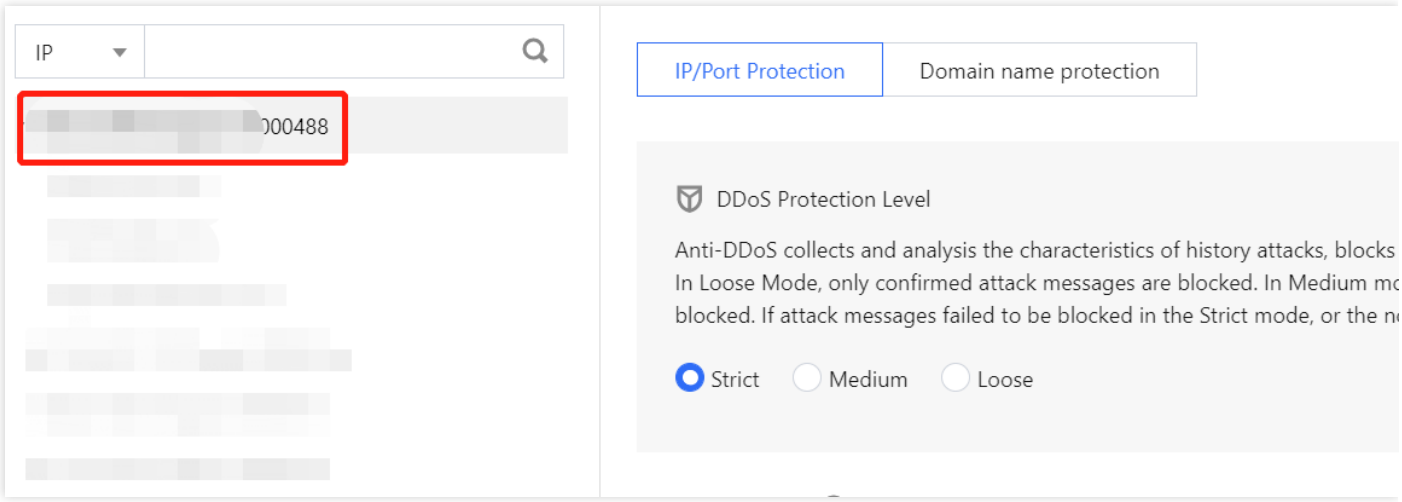
You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Note：
The IP blocklist/allowlist will take effect after being created.

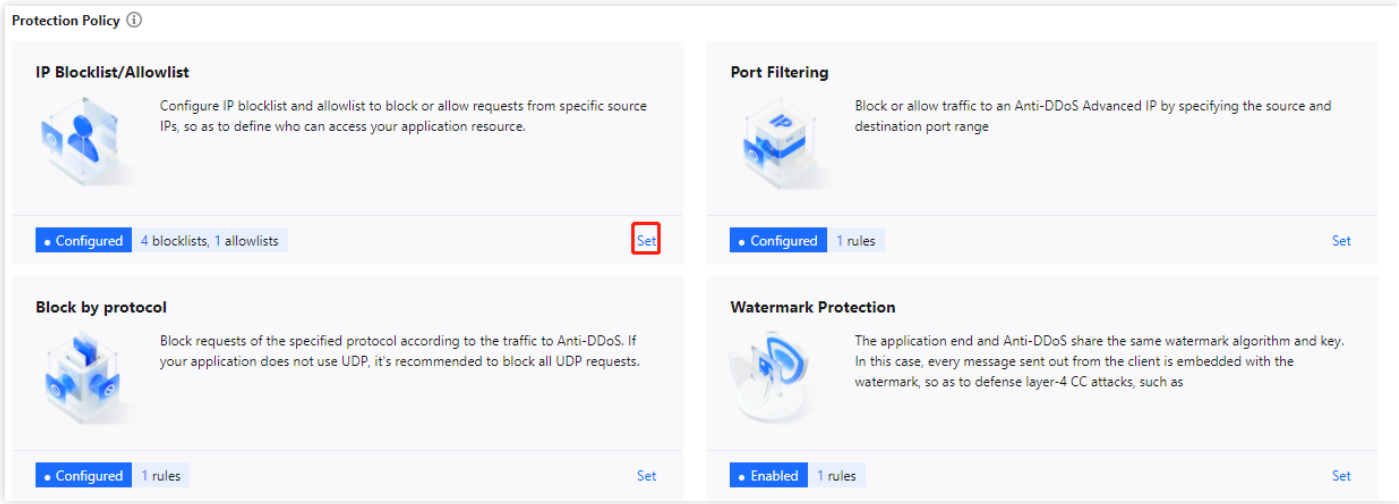
- The allowed IPs will be allowed to access resources without being filtered by any protection policy.
- The access requests from the blocked IPs will be directly denied.

Directions

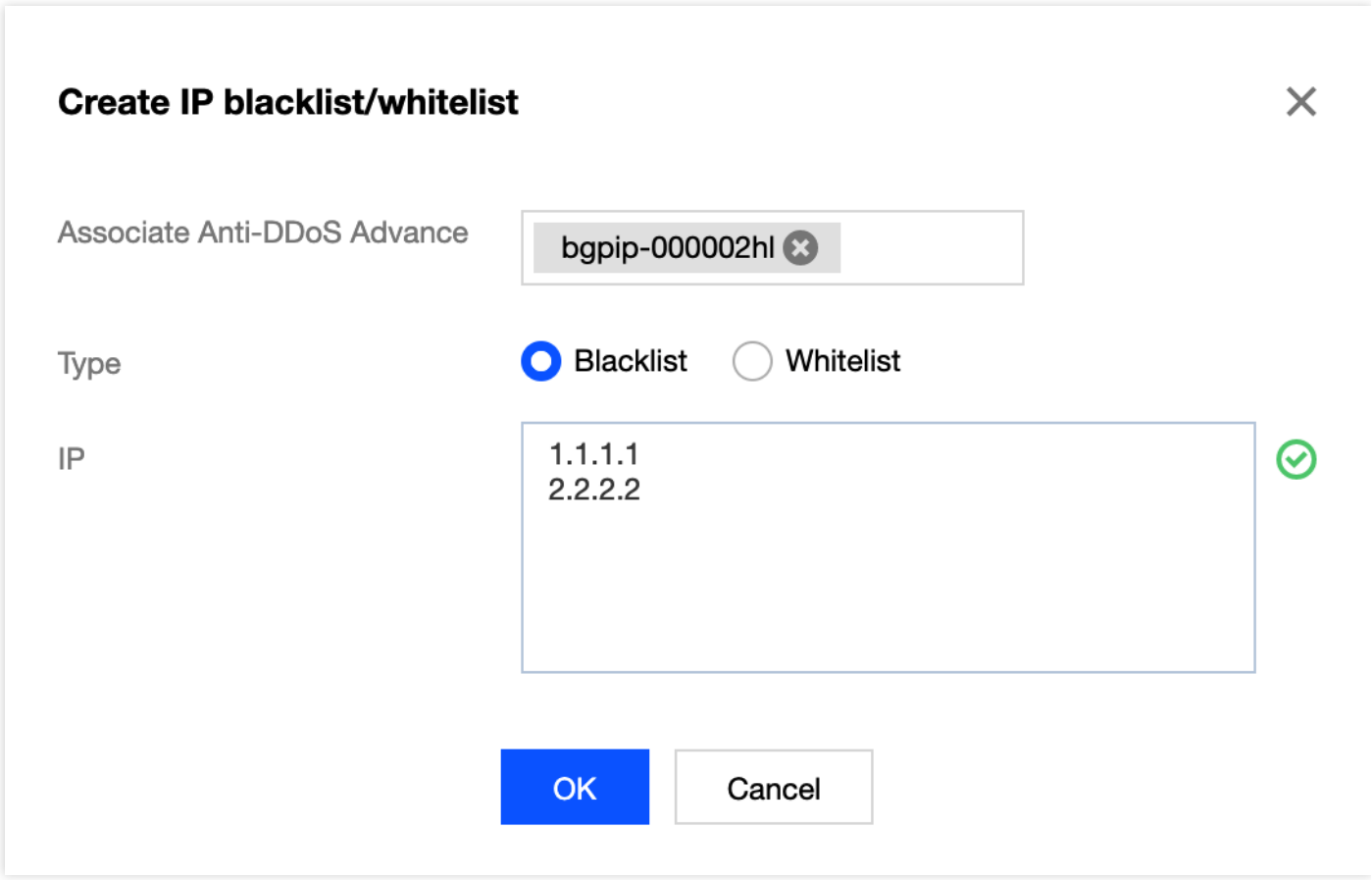
1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **DDoS Protection** tab.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".



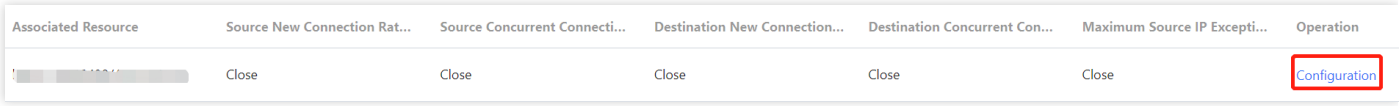
3. Click **Set** in the "IP blocklist/allowlist" section.



4. Click **Create**. In the pop-up window, tick **Blocklist** or **Allowlist** as the type, enter the target IP, and click **OK**.



5. (Optional) After the rule is created, it is added to the rule list. To delete it, click **Delete** in the "Operation" column on the right.



Associated Resource	Source New Connection Rat...	Source Concurrent Connecti...	Destination New Connection...	Destination Concurrent Con...	Maximum Source IP Excepti...	Operation
[redacted]	Close	Close	Close	Close	Close	Configuration

Port Filtering

Last updated：2022-03-11 12:28:20

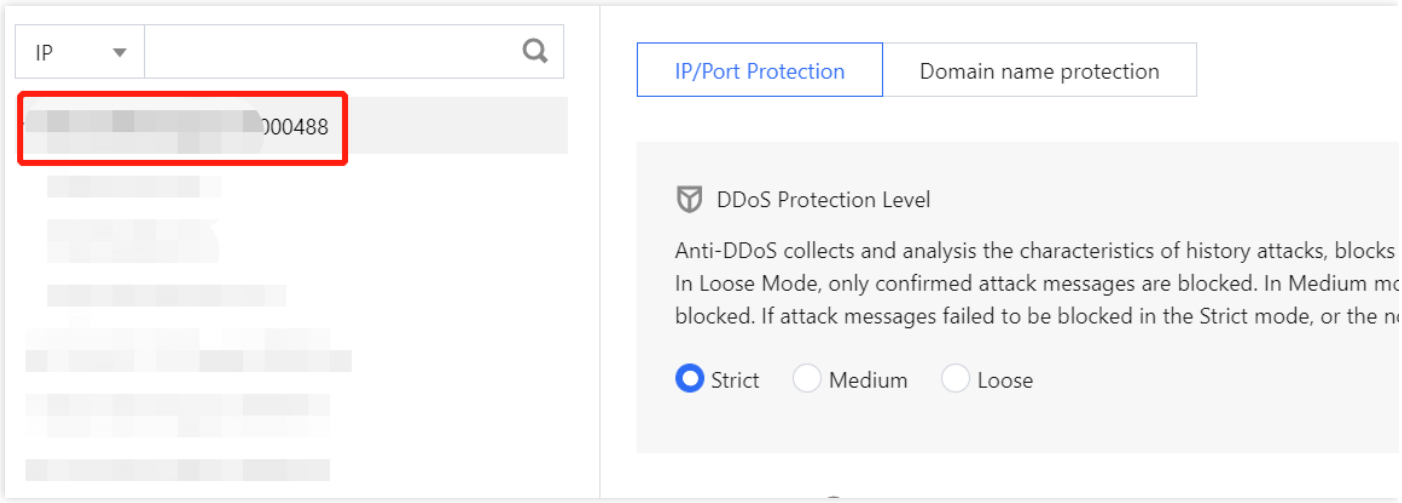
Anti-DDoS Advanced enables you to block or allow inbound traffic by ports. With port filtering enabled, you can customize port settings against inbound traffic, including the protocol type, source port and destination port ranges and set the protection action (allow/block/discard) for the matched rule.

Prerequisites

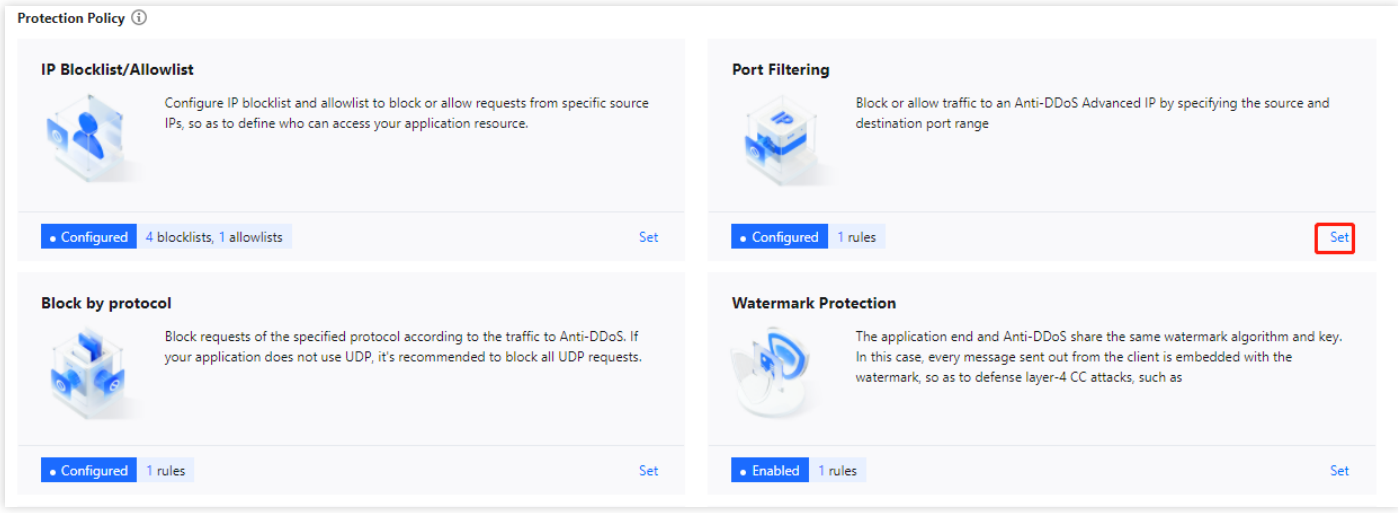
You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **DDoS Protection** tab.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".



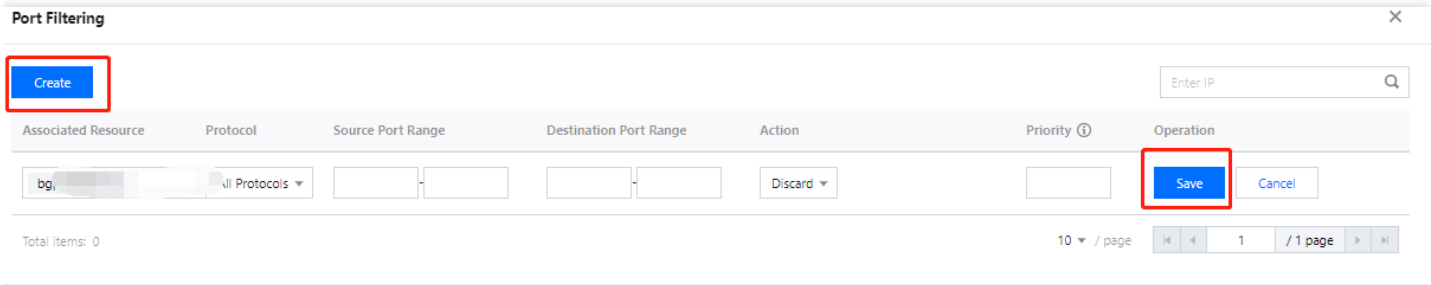
3. Click **Set** in the **Port Filtering** section to enter the port filtering page.



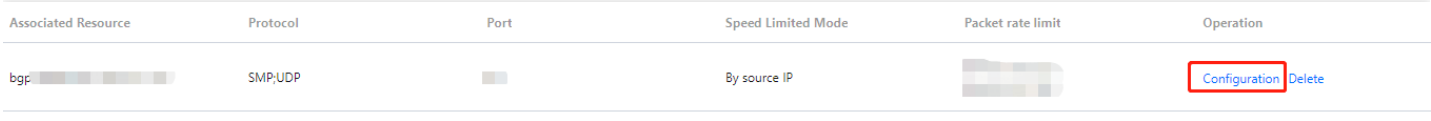
4. Click **Create**, enter the required fields based on the action you select, and then click **Save**.

Note：

- Multiple instances can be created at a time. For instances without protected resources, you cannot create rules.
- For **Priority**, enter an integer between 1-1000. A rule with a lower number has higher priority and is listed higher. Default: 10.



6. After the rule is created, it is added to the rule list. You can click **Configuration** on the right of the rule to modify it.



Regional Blocking

Last updated：2022-03-11 12:28:20

This feature allows you to block traffic from source IP addresses in specific geographic locations at the cleansing node, with just one click. You can block traffic from whatever regions or countries you need.

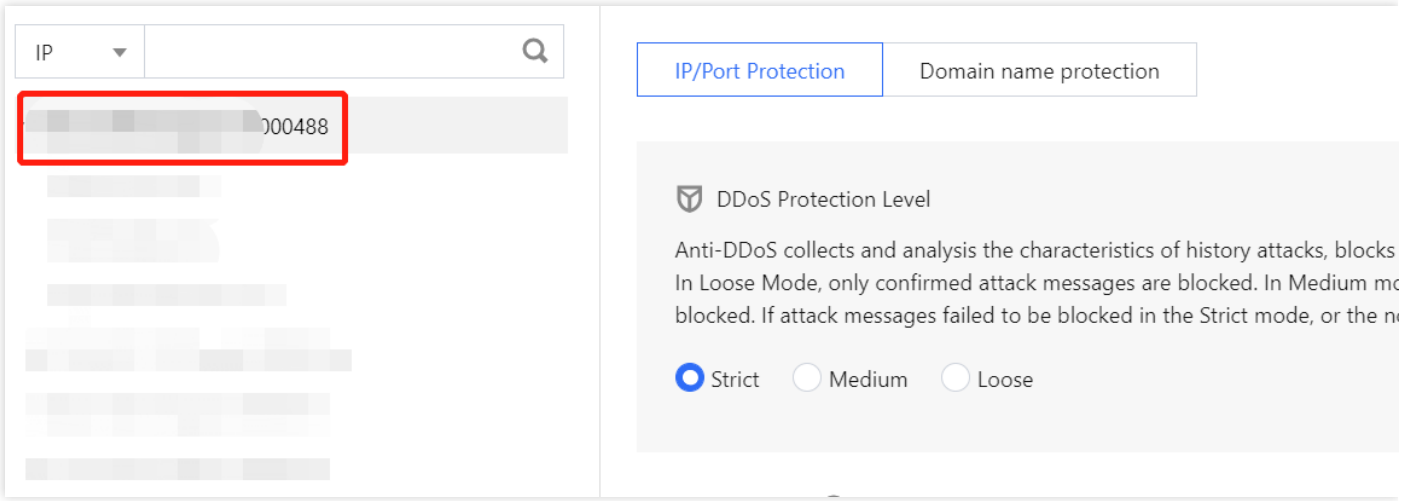
> Note：
> After you configure the regional blocking setting, attack traffic targeting the region will still be recorded but will not be allowed to your real server.

Prerequisites

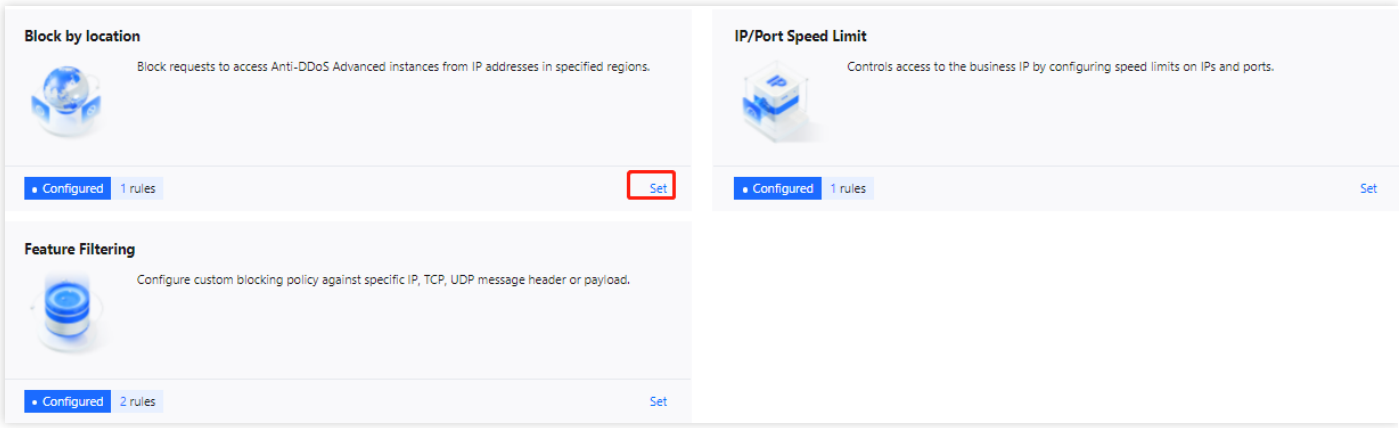
You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

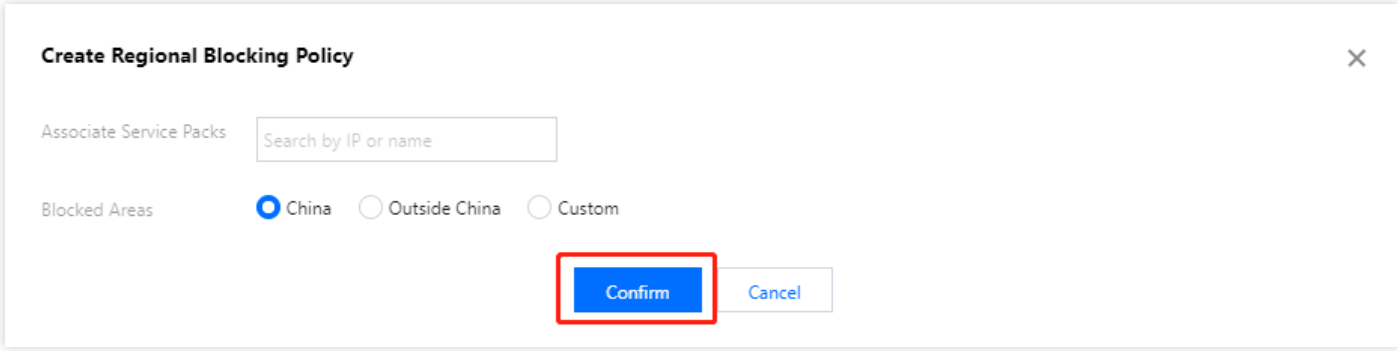
1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **DDoS Protection** tab.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".



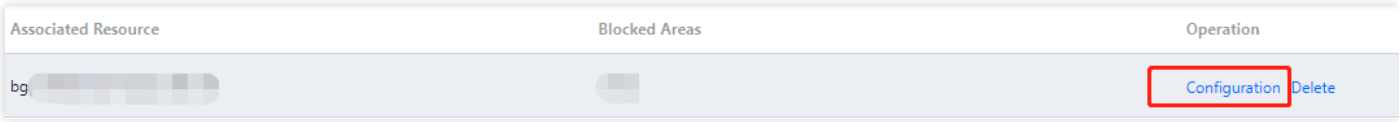
3. Click **Set** in the **Block by Location** section for configuration.



4. Click **Create**.
5. In the pop-up window, select a region to block and click **OK**.



6. Now the new rule is added to the list. You can click **Configuration** on the right of the rule to modify it.



IP and Port Rate Limiting

Last updated：2022-03-11 12:28:20

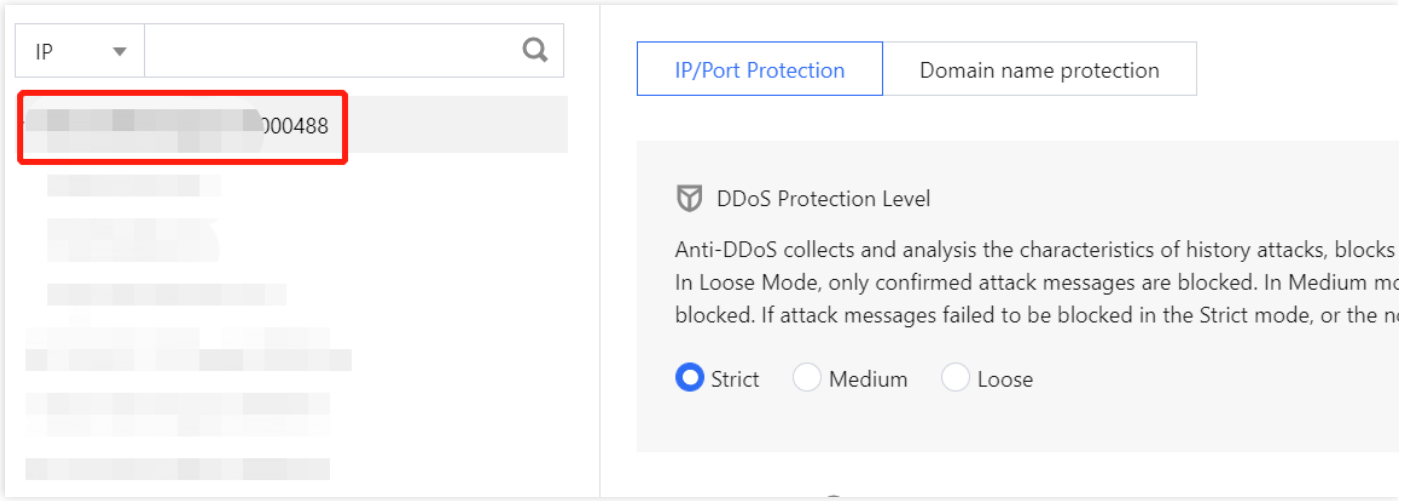
Anti-DDoS Advanced allows you to limit traffic rate for application IPs and ports.

Prerequisites

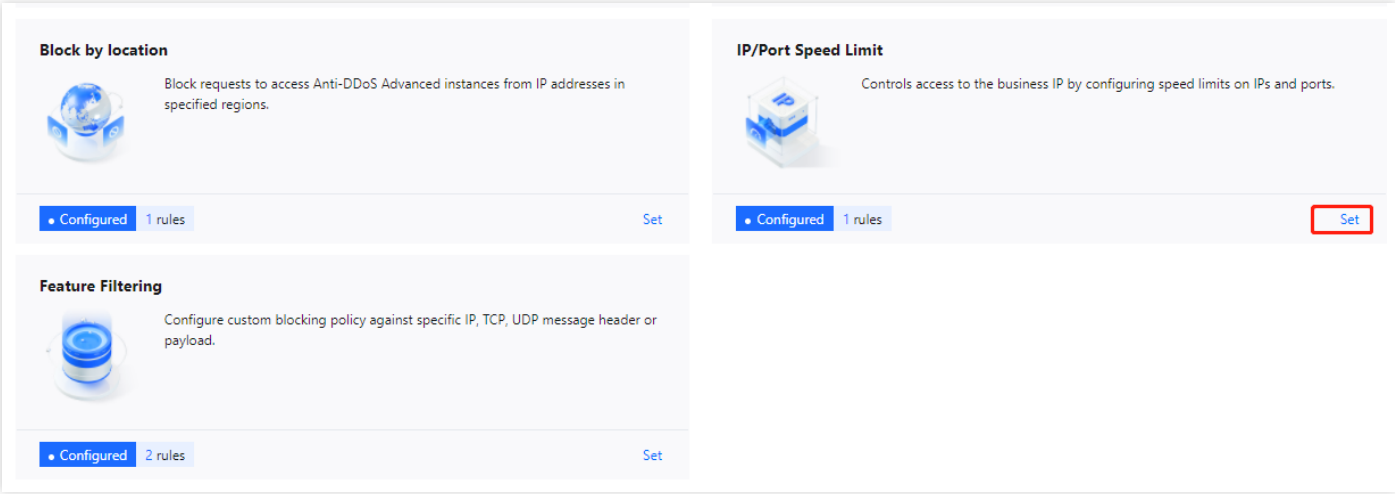
You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

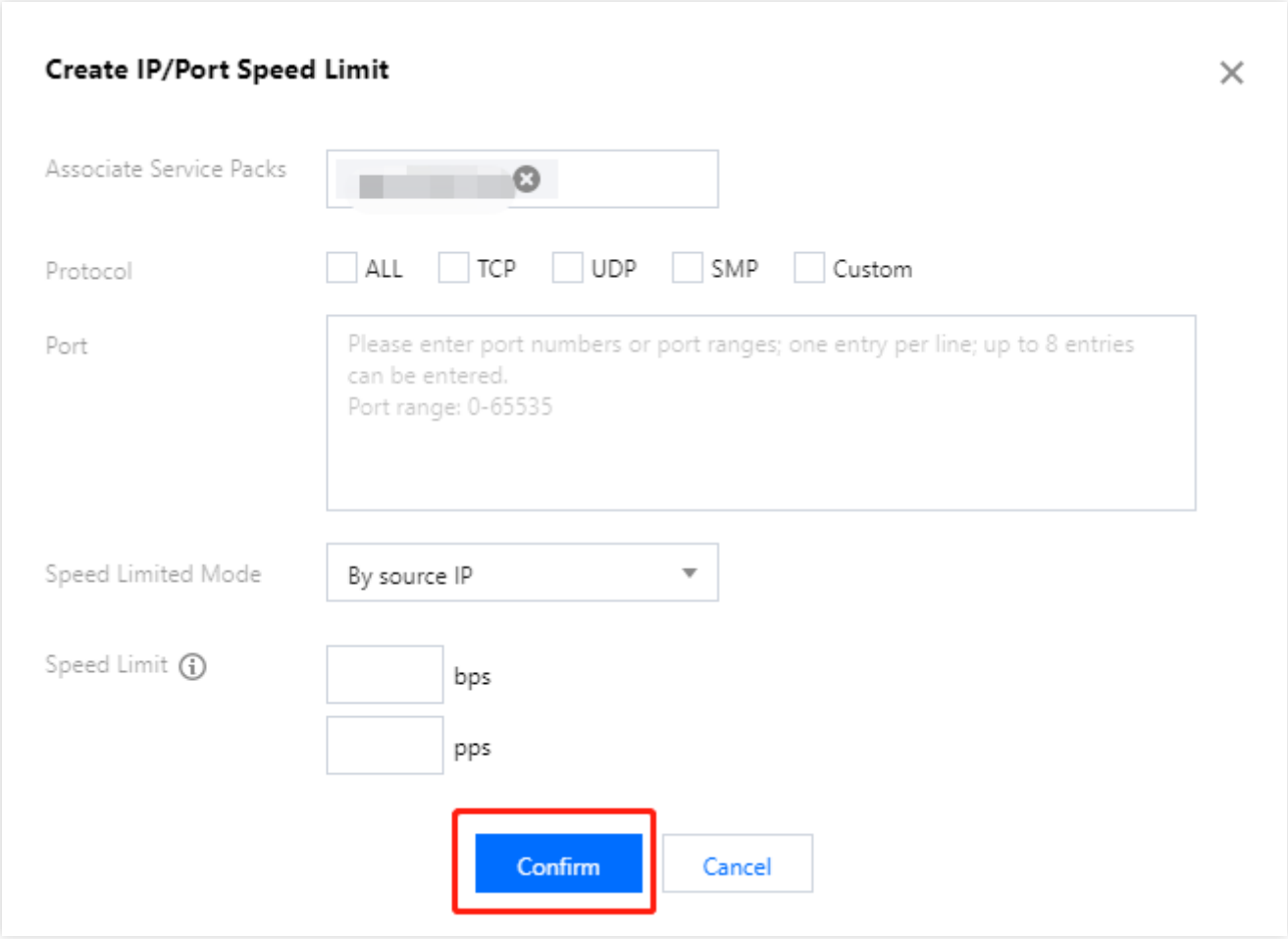
1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **DDoS Protection** tab.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".



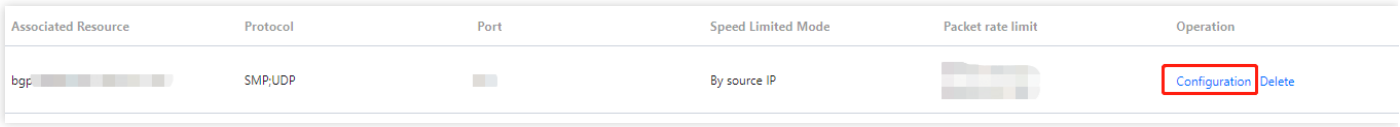
3. Click **Set** in the **IP/Port Speed Limit** section.



4. Click **Create**.
5. In the pop-up window, select a protocol for the port you set, set a rate limit, and then click **OK**.



6. After the rule is created, it is added to the list. You can click **Configuration** on the right of the rule to modify it.



Connection Attack Protection

Last updated：2022-06-10 14:12:06

Anti-DDoS Advanced can automatically trigger blocking policies facing abnormal connections. With **Maximum Source IP Exceptional Connections** enabled, a source IP that frequently sends a large number of messages about abnormal connection status will be detected and added to the blocklist. The source IP will be accessible after being blocked for 15 minutes. You can set the following configurations as needed:

Note：

- **Source New Connection Rate Limit**: It limits the rate of new connections from source ports.
- **Source Concurrent Connection Limit**: It limits the number of active TCP connections from source addresses at any one time.
- **Destination New Connection Rate Limit**: It limits the rate of new connections from destination IP addresses and destination ports.
- **Destination Concurrent Connection Limit**: It limits the number of active TCP connections from destination IP addresses at any one time.
- **Maximum Source IP Exceptional Connections**: It limits the maximum number of abnormal connections from source IP addresses.

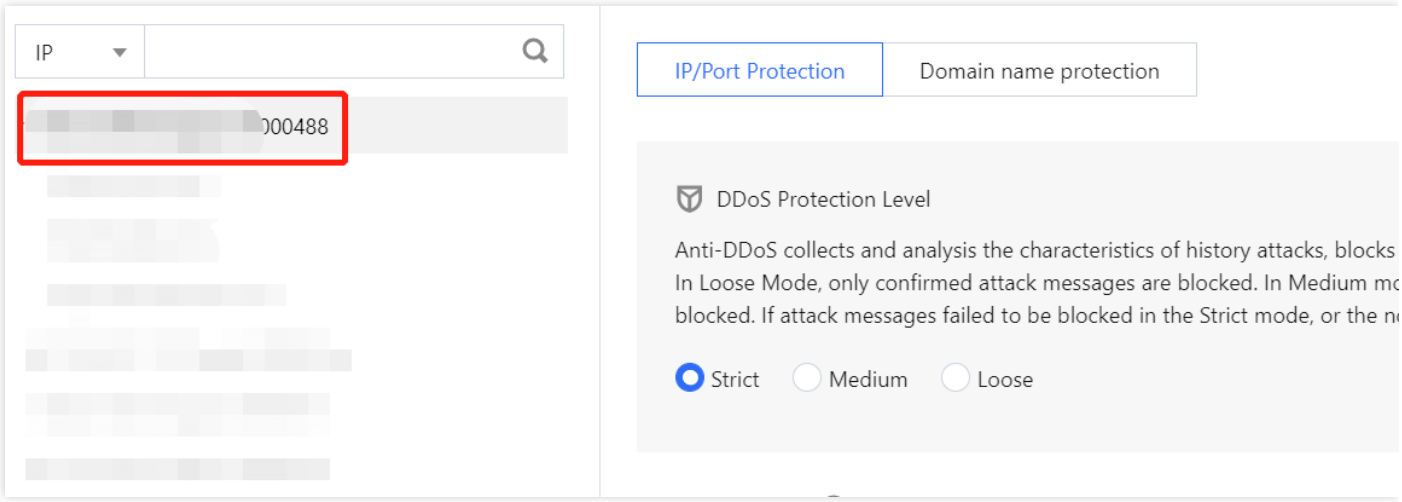
Prerequisites

You have purchased an Anti-DDoS Advanced instance and set the object to protect.

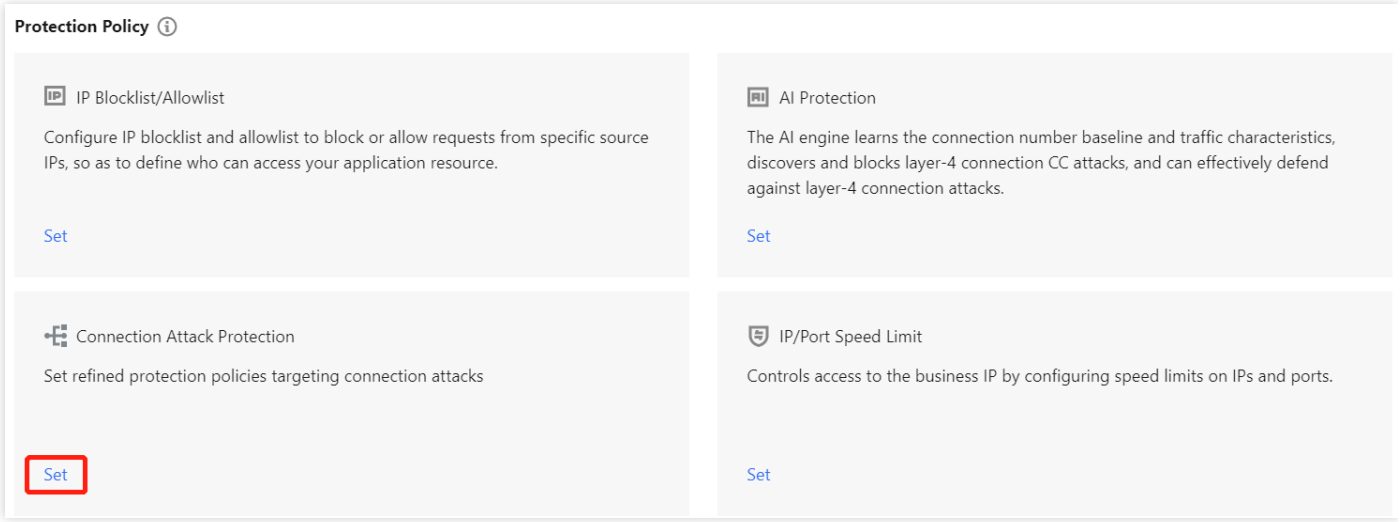
Directions

1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **DDoS Protection** tab.

2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgpip-xxxxxx".

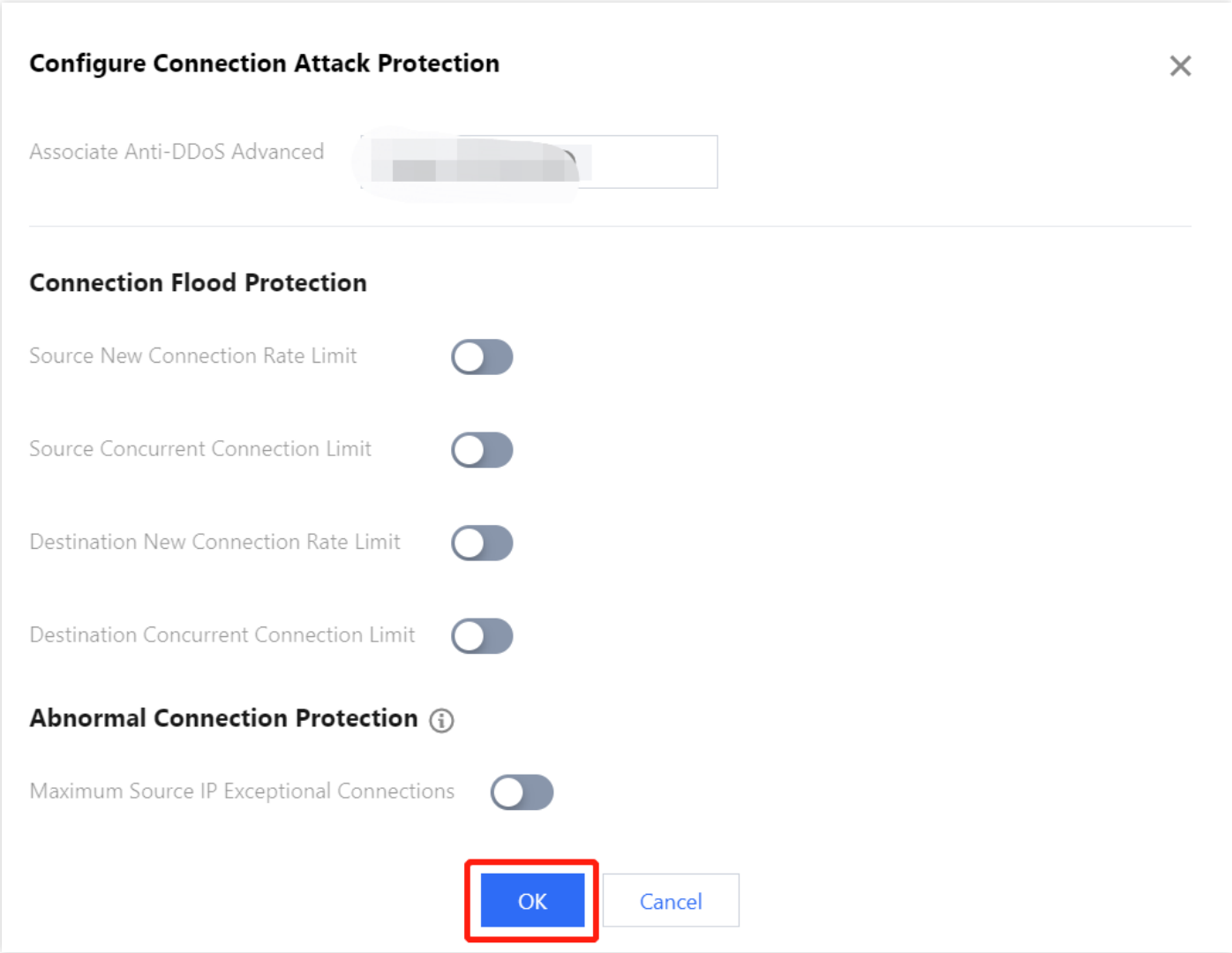


3. Click **Set** in the **Connection Attack Protection** to enter the configuration page.

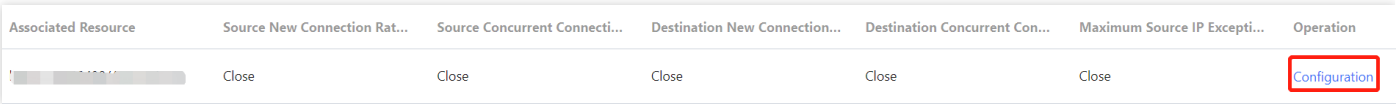


4. Click **Create** to create a connection attack protection rule.

5. In the pop-up window, enable **Abnormal Connection Protection**, and click **OK**.



6. After the rule is created, it is added to the list. You can click **Configuration** on the right of the rule to modify it.



CC protection
Protection Level and Cleansing Threshold

Last updated：2022-03-02 13:25:43

Protection Description

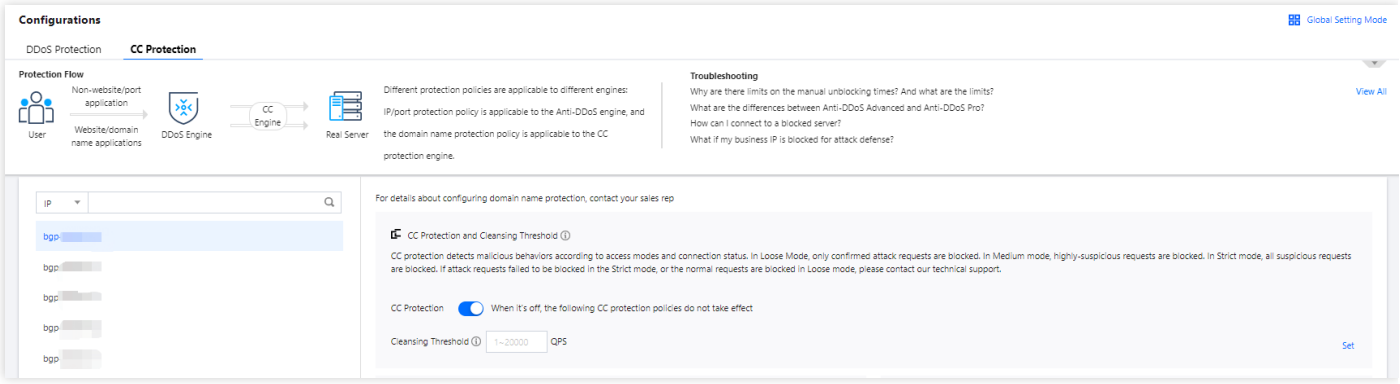
"CC Protection" identifies and blocks CC attacks based on access attributes and connection status. It provides scenario-specific configurations to create protection rules, helping secure your business. It also supports the cleaning threshold setting.

Prerequisites

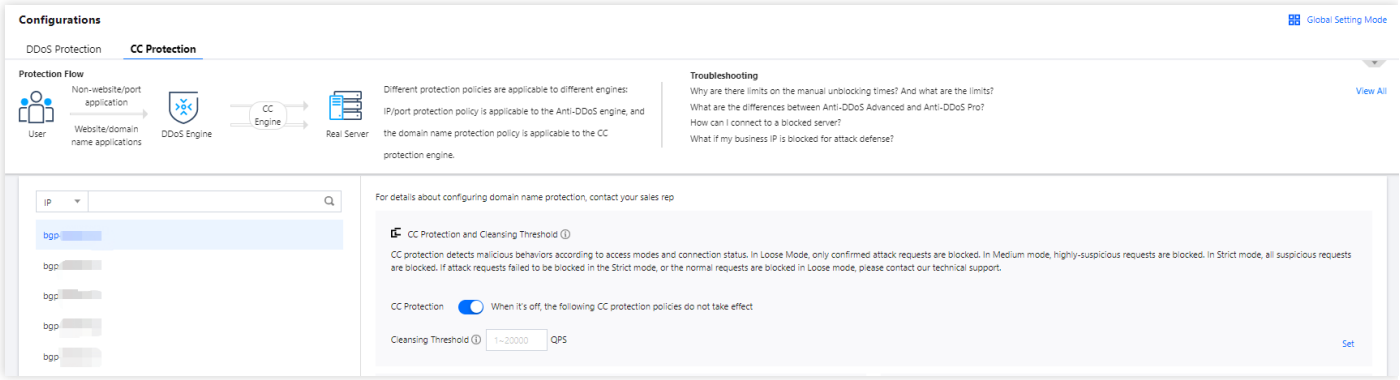
You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **CC Protection** tab.
2. Select a domain name from the IP list.



3. To enable CC protection in the "CC Protection and Cleansing Threshold" section, click  and set a cleansing threshold.



Note：

- This switch controls wether to enable CC protection. Only when it is on, all the CC protection policies take effect.
- The cleansing threshold is the threshold for Anti-DDoS services to start cleansing traffic. If the number of HTTP requests sent to the specified domain name exceeds the threshold, CC protection will be triggered.
- If the protection is enabled, your Anti-DDoS Advanced instance will use the default cleansing threshold after your business is connected, and the system will generate a baseline based on historical patterns of your business traffic. You can also set the cleansing threshold for your business needs.
- If you have a clear concept about the threshold, set it as required. Otherwise please leave it to the default value. Anti-DDoS will automatically learn through AI algorithms and generate the default threshold for you.

Intelligent CC Protection

Last updated：2023-04-28 16:48:50

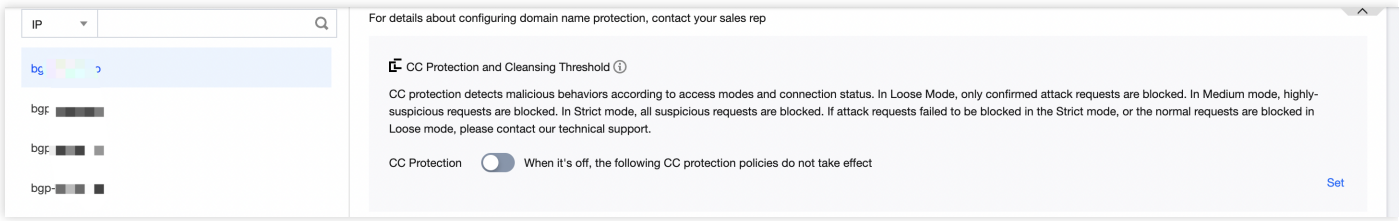
Intelligent CC protection is an AI-powered protection feature leveraging Tencent Cloud's big data capability. It provides a dynamic protection model to auto-generate rules for detecting and blocking malicious attacks based on website traffic patterns and algorithm-utilized attack analysis.

Prerequisites

- You have purchased an Anti-DDoS Advanced instance and set the object to protect.
- Only rules configured for instances accessing via domain names take effect.

Directions

1. Log in to the Anti-DDoS console. Select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **CC Protection** tab.
2. Select a domain name from the IP list on the left.

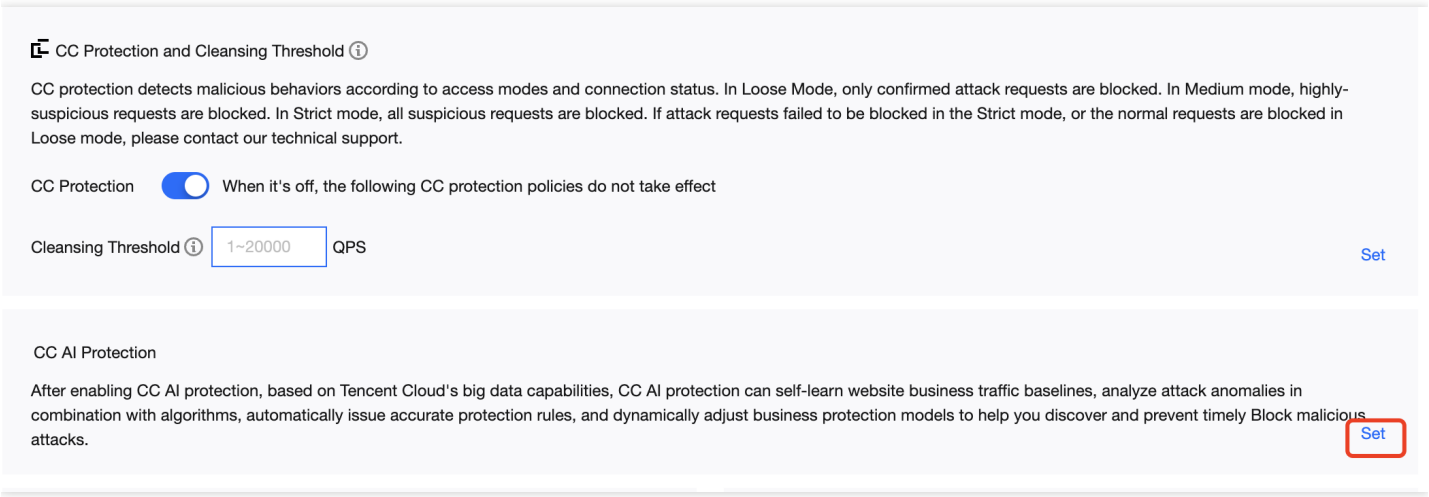


3. In the "CC Protection and Cleansing Threshold" card, click  and set a cleansing threshold before enabling intelligent CC protection.

Note：

- The cleansing threshold is the threshold for Anti-DDoS services to start cleansing traffic. If the number of HTTP requests sent to the specified domain name exceeds the threshold, CC protection will be triggered.
- If the IP bound to the Anti-DDoS Pro instance is from WAF, you need to first enable CC protection for the IP in the WAF console. For more information, see CC Protection Rules.

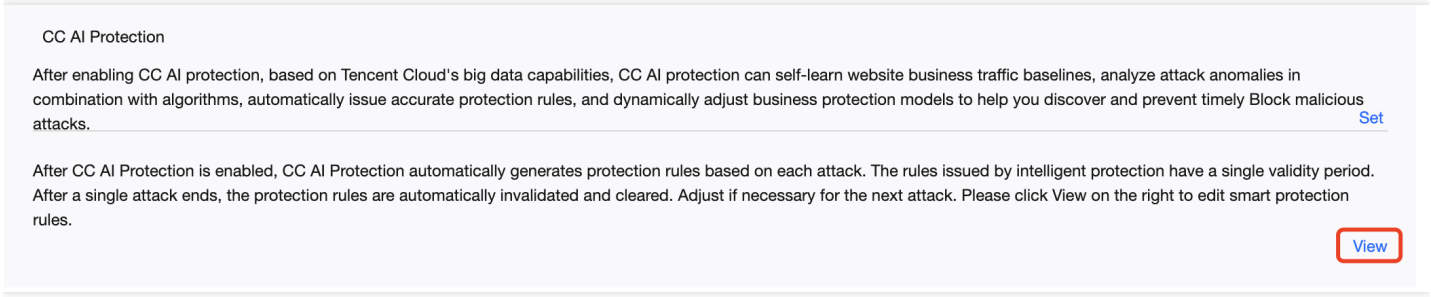
4. In the **Intelligent CC protection** card, toggle on  the switch.



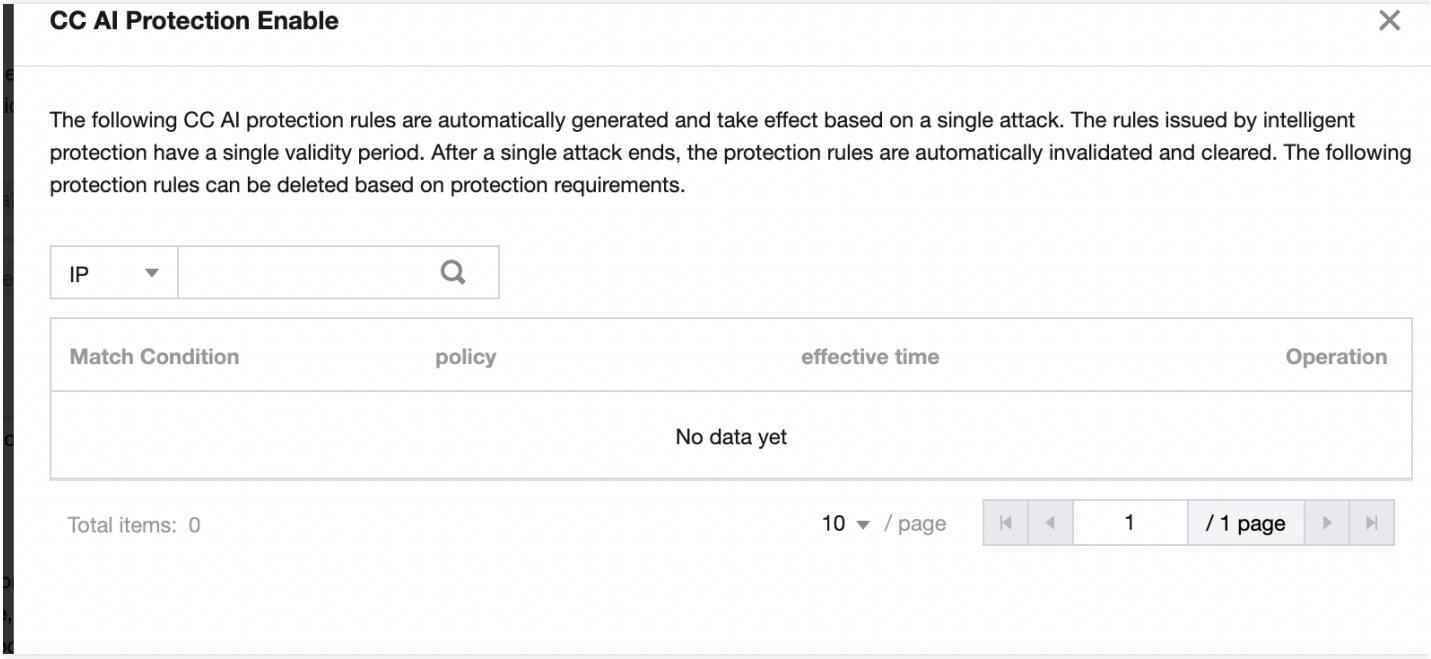
5. Click **View** to view the auto-generated protection rules. You can make changes to these rules if necessary.

Note：

- When intelligent CC protection is enabled, the protection rules are auto-generated when an attack occurs.
- Protect mode: Apply auto-generated protection rules to defend against each specific attack. After the attack ends, the rules are automatically deleted.
- Observe mode: Attacks are observed only.



6. To delete a rule, click **Delete** on the right of the rule you want to remove.



Precise Protection

Last updated：2022-12-21 17:50:10

Use Cases

Anti-DDoS supports precise protection for connected web applications. With the precise protection, you can configure protection policies combining multiple conditions of common HTTP fields, such as URI, UA, Cookie, Referer, and Accept to screen access requests. For the requests matched the conditions, you can configure CAPTCHA to verify the requesters or a policy to automatically drop or allow the requests. Precise protection is available for policy customization in various use cases to precisely defend against CC attacks.

The match conditions define the request characteristics to be checked, i.e., the attribute characteristics of the HTTP field in a request. Precise protection supports checking the HTTP fields below:

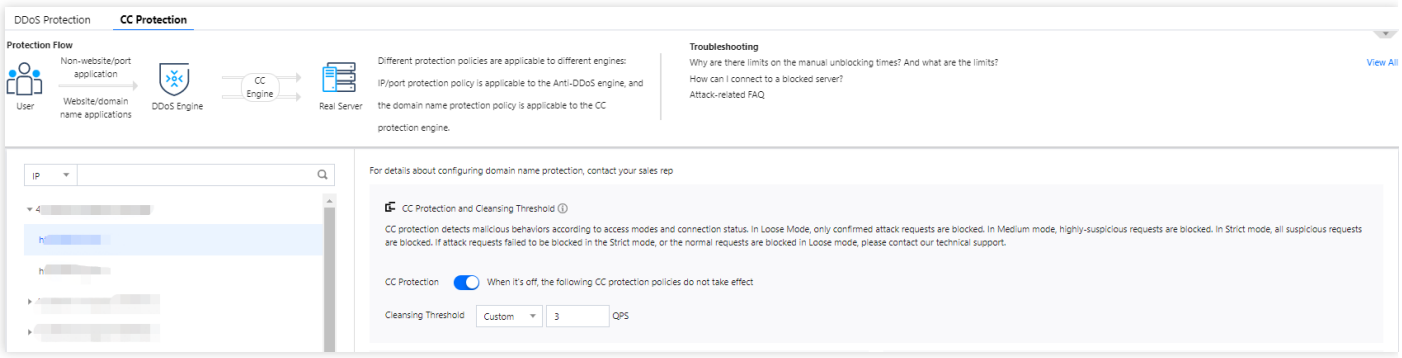
Match Field	Field Description	Logic
URI	The URI of an access request.	Equals to, includes, or does not include.
UA	The identifier and other information of the client browser that initiates an access request.	Equals to, includes, or does not include.
Cookie	The cookie information in an access request.	Equals to, includes, or does not include.
Referer	The source website of an access request, from which the access request is redirected.	Equals to, includes, or does not include.
Accept	The data type to be received by the client that initiates the access request.	Equals to, includes, or does not include.

Prerequisites

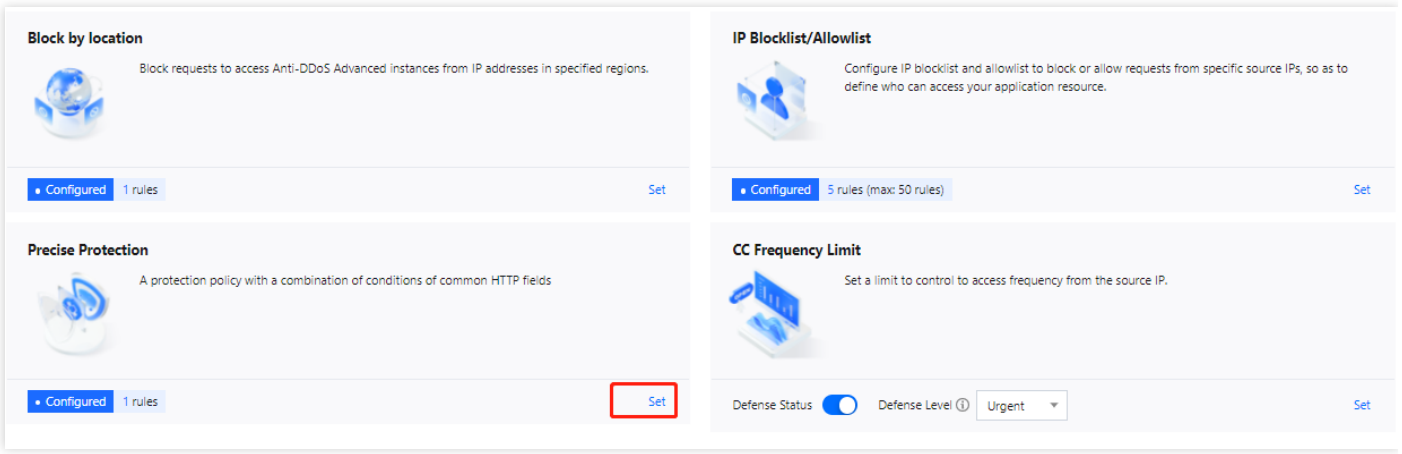
You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

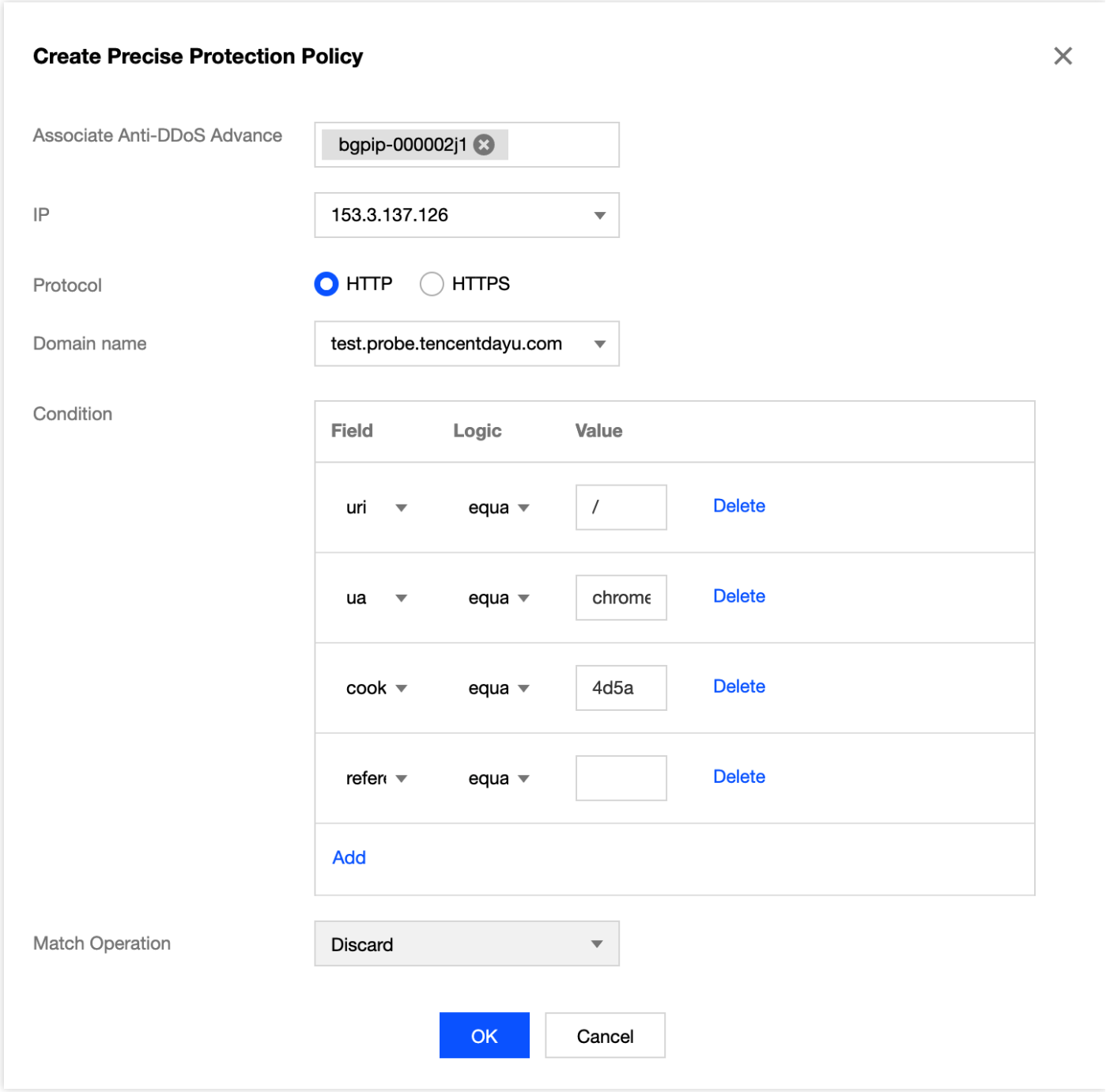
1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **CC Protection** tab.
2. Select a domain name from the IP list on the left.



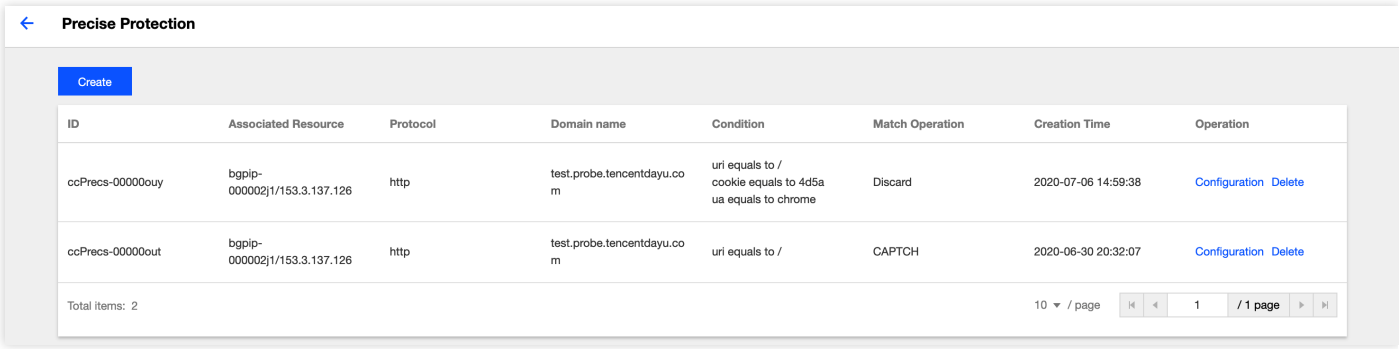
3. Click **Set** in the **Precise Protection** section to enter the rule list.



4. Click **Create** to create a precise protection rule. Fill in the fields and click **OK**.



5. Now the new rule is added to the rule list. You can click **Configuration** on the right of the rule to modify it.



CC Frequency Limit

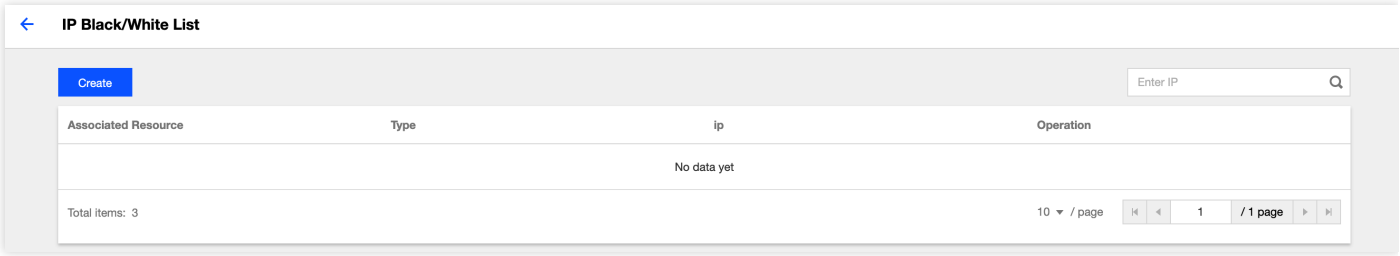
Last updated：2020-07-07 17:19:14

Prerequisites

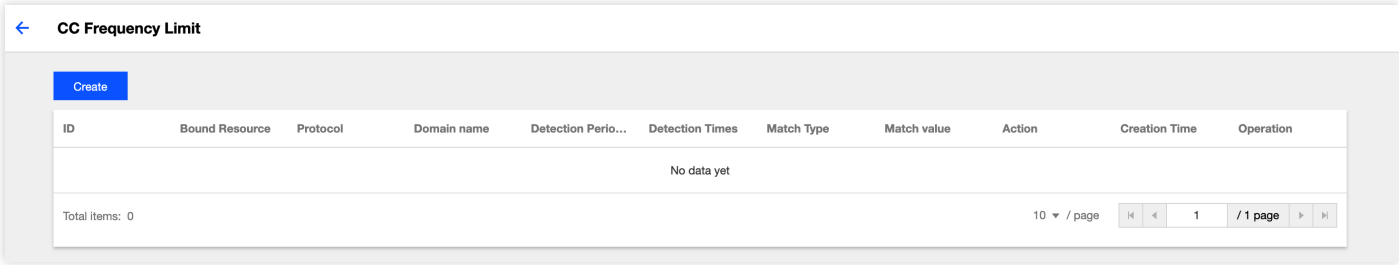
You need to purchase an Anti-DDoS Advanced instance and set the protected object first.

Directions

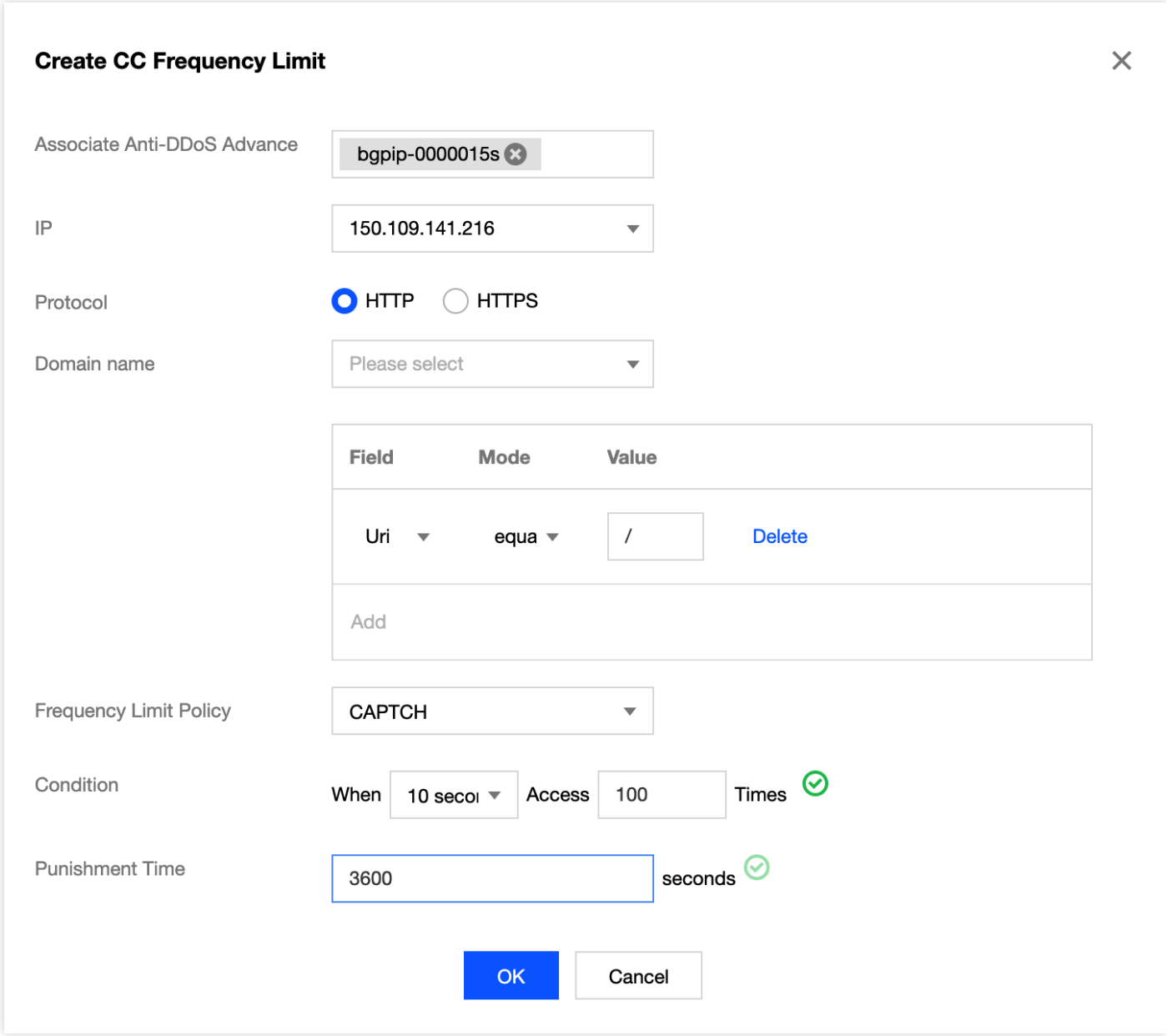
1. Log in to the new Anti-DDoS Advanced Console and select **Protection Configuration** on the left sidebar.
2. Select a domain name under the ID of an Anti-DDoS Advanced instance in the list on the left; for example, select "212.64.xx.xx bgpip-000002je" > "http:80" > "www.xxx.com".



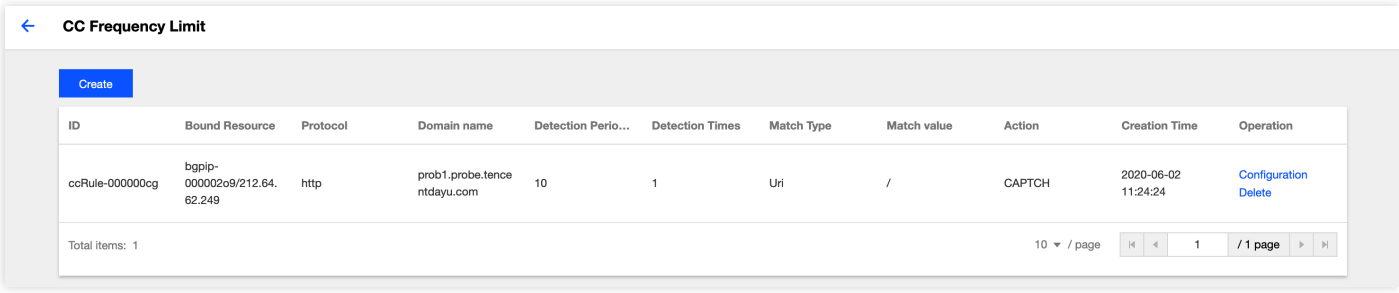
3. Click **Set** in the "CC Frequency Limit" block on the right to enter the frequency limit rule list.



4. Click **Create** to create a frequency limit rule, fill in relevant fields, and click **OK**.



5. After the creation is completed, a frequency limit rule will be added to the frequency limit list. You can modify the rule by clicking **Configure** in the "Operation" column on the right.



Regional Blocking

Last updated：2022-03-11 12:28:20

Anti-DDoS Advanced allows you to block website access requests from source IP addresses in specific geographic locations, with just one click. You can block all website access requests from whatever regions or countries you need.

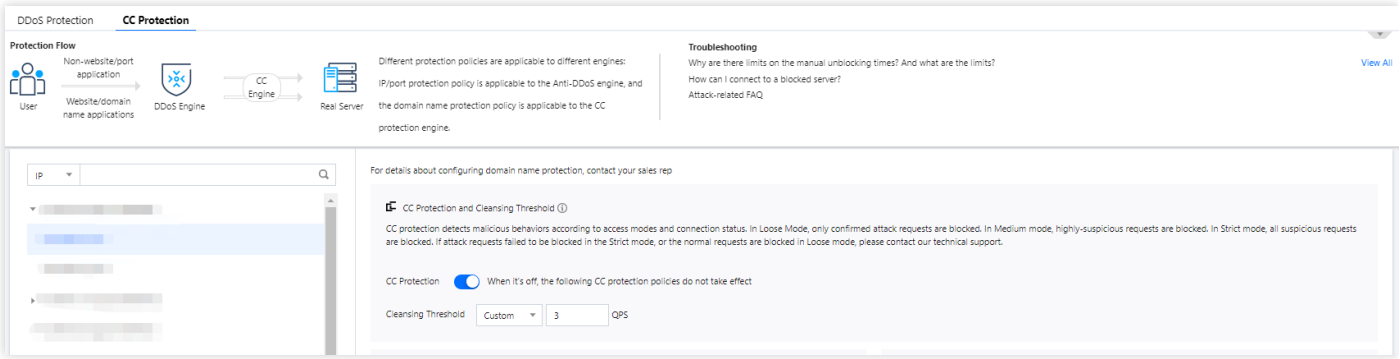
> Note：
> After you configure the regional blocking setting, attack traffic targeting the region will still be recorded but will not be allowed to your real server.

Prerequisites

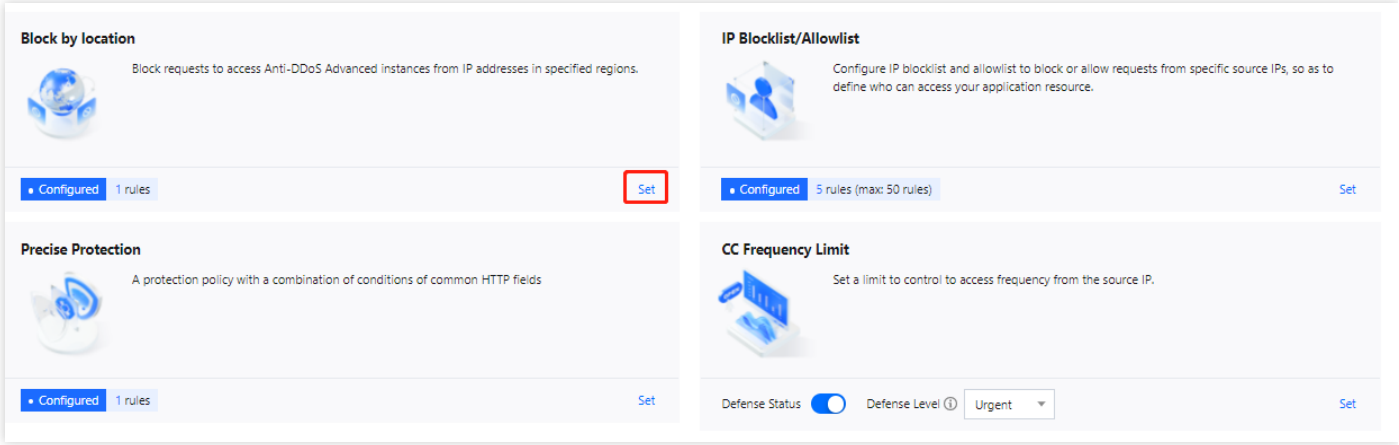
You have purchased an Anti-DDoS Advanced instance, set your target to protect, and connected to domain names.

Directions

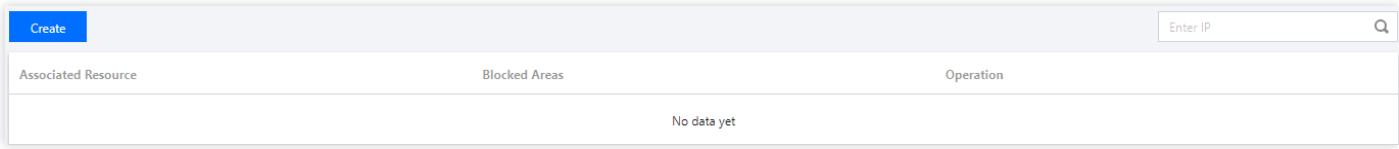
1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **CC Protection** tab.
2. Select a domain name from the IP list on the left.



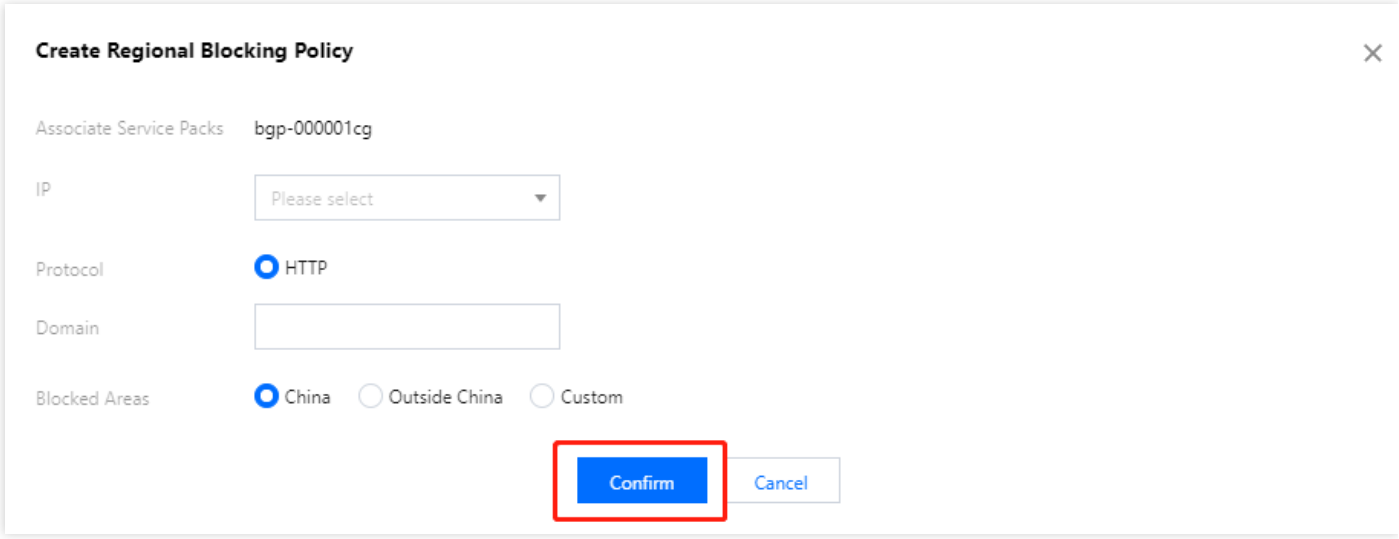
3. Click **Set** in the **Block by Location** section for configuration.



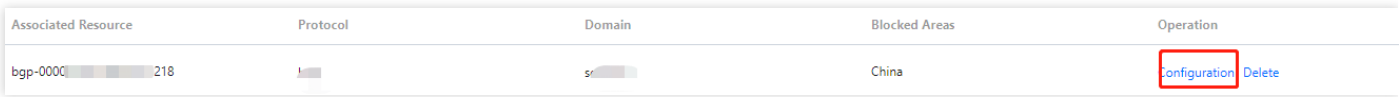
4. Click **Create**.



5. In the pop-up dialog, select an IP, a protocol, domain name, and region. Click **OK**.



6. Now the new rule is added to the list. You can click **Configuration** on the right of the rule to modify it.



IP Blocklist/Allowlist

Last updated：2022-03-02 13:25:43

Anti-DDoS Advanced supports IP blocklist and allowlist configurations to block and allow IPs connected to Anti-DDoS Advanced, restricting the users from accessing your resources. For the allowed IPs, they are allowed to access without being filtered by any protection policy; while the access requests from the blocked IPs are directly denied.

Note：
The IP blocklist and allowlist filtering takes effect only when your business is under CC attacks.

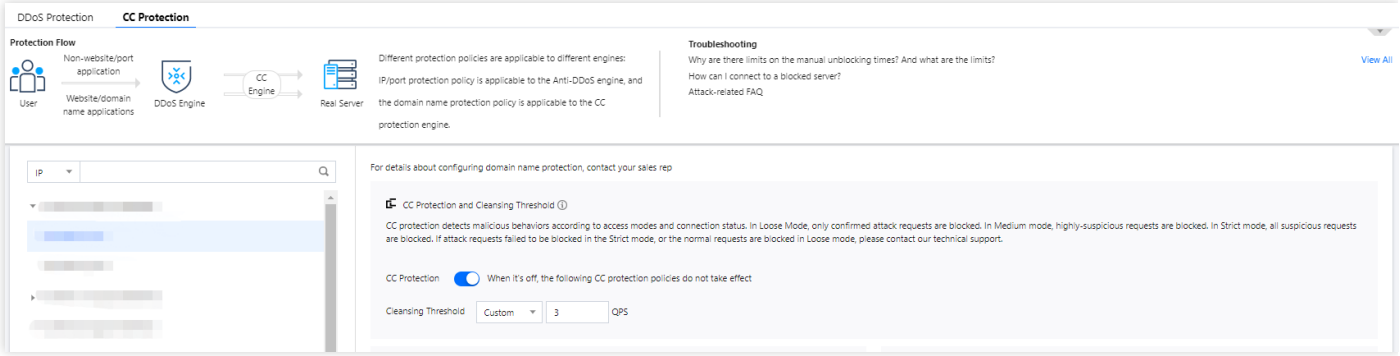
- The allowed IPs will be allowed to access resources without being filtered by any protection policy.
- The access requests from the blocked IPs will be directly denied.

Prerequisites

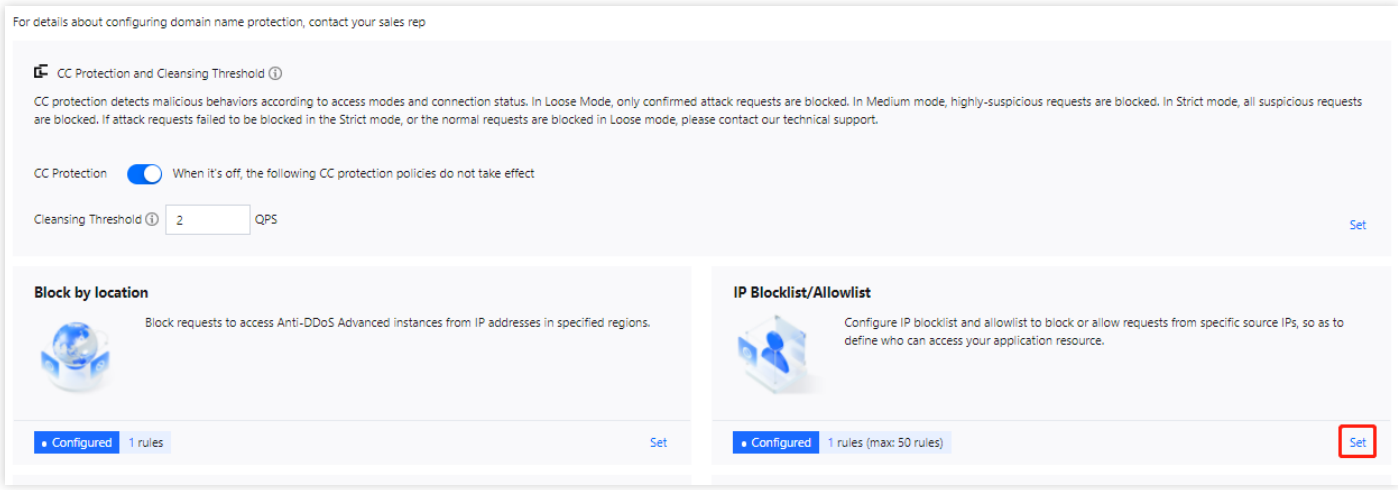
You have purchased an Anti-DDoS Advanced instance and set the object to protect.

Directions

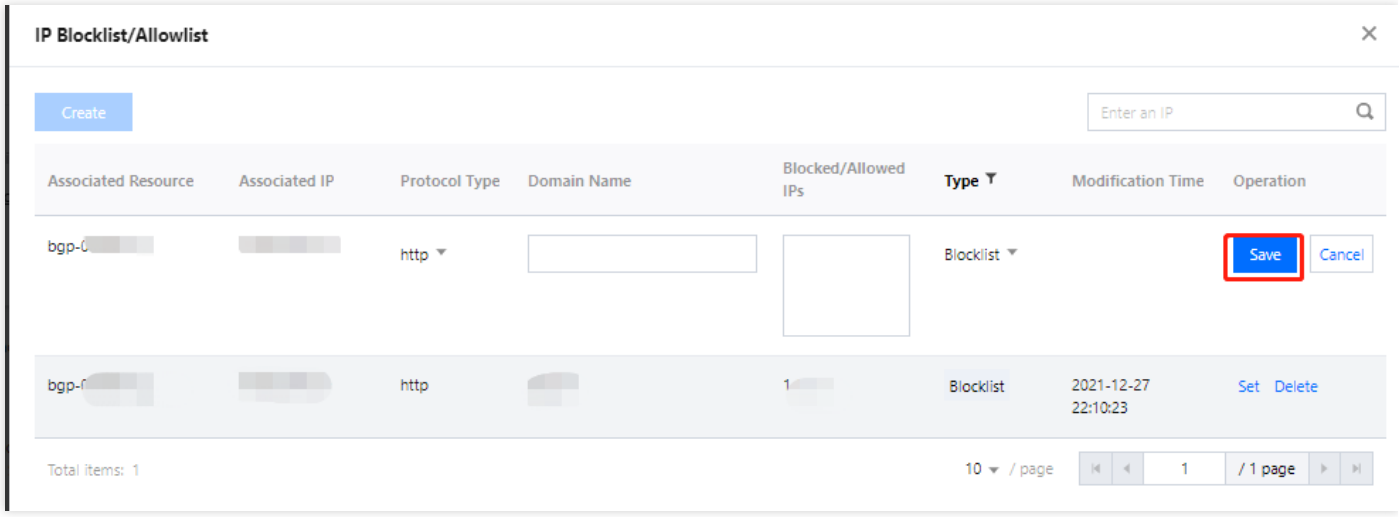
1. Log in to the Anti-DDoS console and select **Anti-DDoS Advanced (New)** > **Configurations** on the left sidebar. Open the **CC Protection** tab.
2. Select a domain name from the IP list on the left.



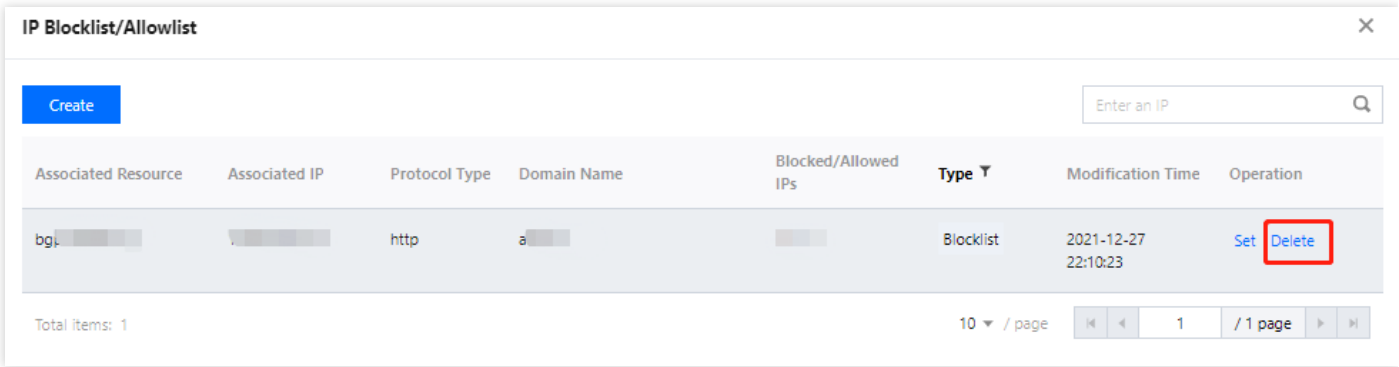
3. Click **Set** on the **IP Blocklist/Allowlist** section.



4. Click **Create**, and enter the required fields before you click **Save**.



5. Now the rule is added to the list. You can click **Delete** on the right of the rule to delete it.



Business Connection
Port Connection

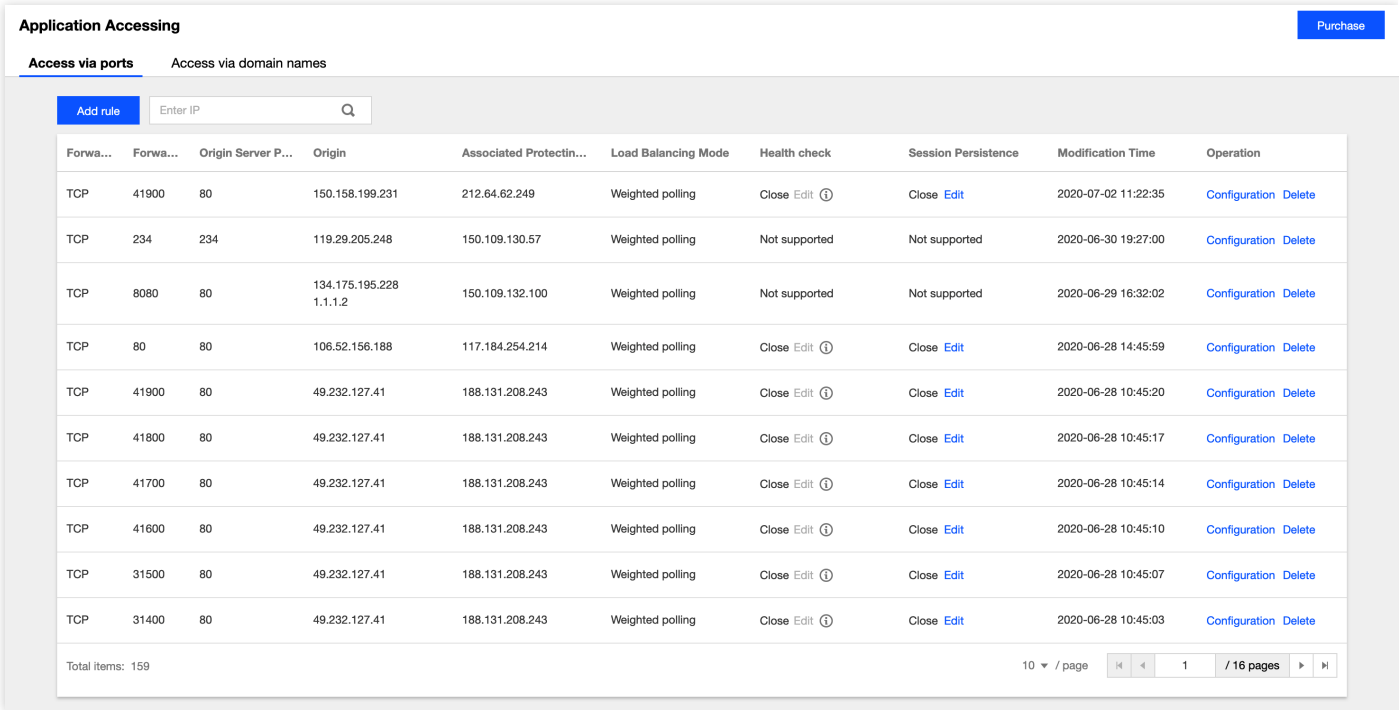
Last updated：2023-04-28 16:48:50

Note：
Note that the DNS address should be changed to the CNAME address provided, which will be updated (Non-BGP resources are not supported).

Accessing a Rule

1. Log in to the Anti-DDoS Advanced Console, select **Anti-DDoS Advanced (New)** > **Application Accessing** on the left sidebar, and then open the **Access via ports** tab.

2. Click **Start Access**.



3. On the **Access via Port** page, select an associated instance ID and click **Next: Set Port Parameter**.

> Note：
> You can select multiple instances.

4. Select a forwarding protocol, specify a forwarding port and real server port, and then click **Next: Set Forwarding Method**.

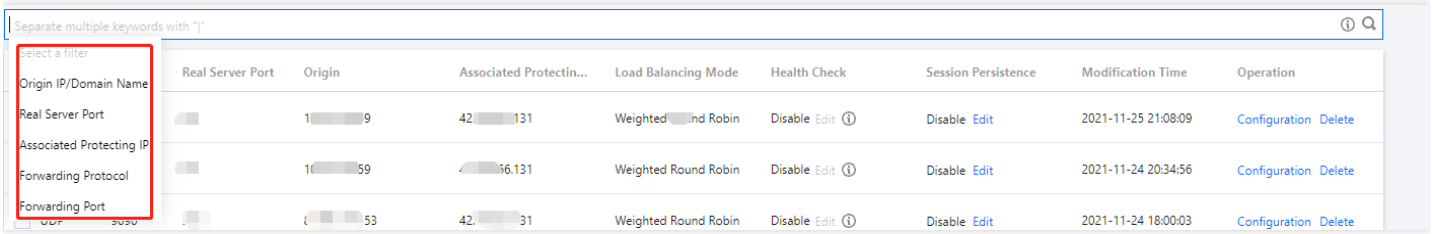
5. Select a forwarding method, specify a "real server IP+port"/real sever domain name, and add an alternate real server and set the weight if you have one. Then click **Next: Modify DNS Resolution**.

> Note：
> - An alternate real server is used when the real server's forwarding fails.
> - If the forwarding port you specify in the second step "Set Port Parameter" is occupied, you cannot proceed to the next step.

6. Click **Complete**.

Querying a Rule

On the Access via ports page, enter a real server IP/domain name, real server port, forwarding protocol/port or an associated instance ID in the search box.



Editing a Rule

1. On the Access via ports page, select a rule you want to edit and click **Configuration**.
2. On the **Configure Layer-4 Forwarding Rule** page, modify parameters and click **OK** to save changes.

Deleting Rules

1. On the Access via ports page, you can delete one or more rules.
   - To delete a rule, select a rule you want to delete. Click **Delete**.
   - To delete multiple rules, select more than one rules you want to delete. Click **Batch Delete**.
2. In the pop-up window, click **Delete**.

Importing a Rule

1. To import multiple rules, you can click **Batch Import** on the Access via ports page.
2. In the **Configure Layer-4 Forwarding Rule** window, enter the rules, and click **OK**.

Exporting a Rule

1. To import multiple rules, you can click **Batch Export** on the Access via ports page.
2. In the **Batch Export Layer-4 Forwarding Rules** window, select the rules you want to export, and click **Copy**.

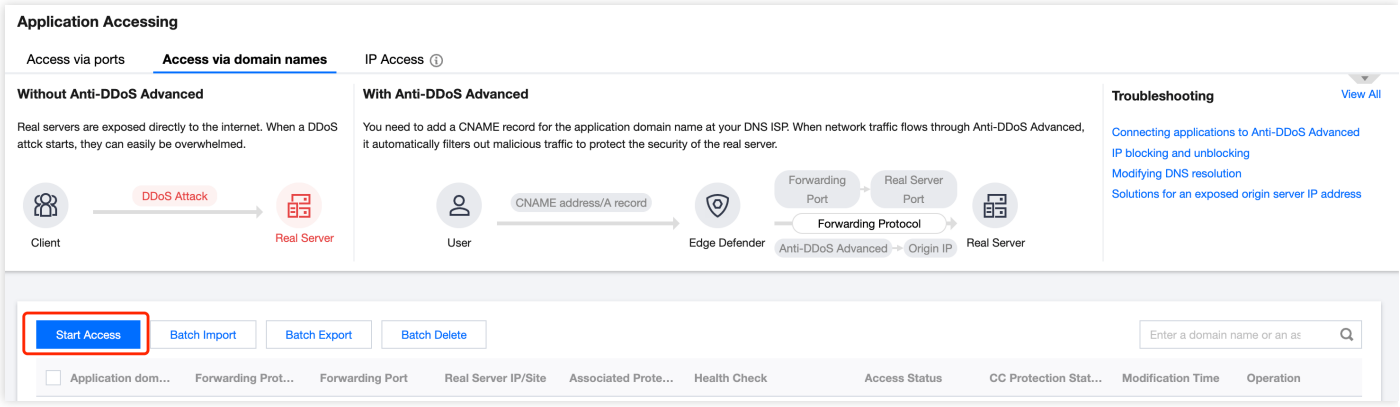
Domain Name Connection

Last updated：2023-04-28 16:48:50

Note：
Note that the DNS address should be changed to the CNAME address provided, which will be updated (Non-BGP resources are not supported).

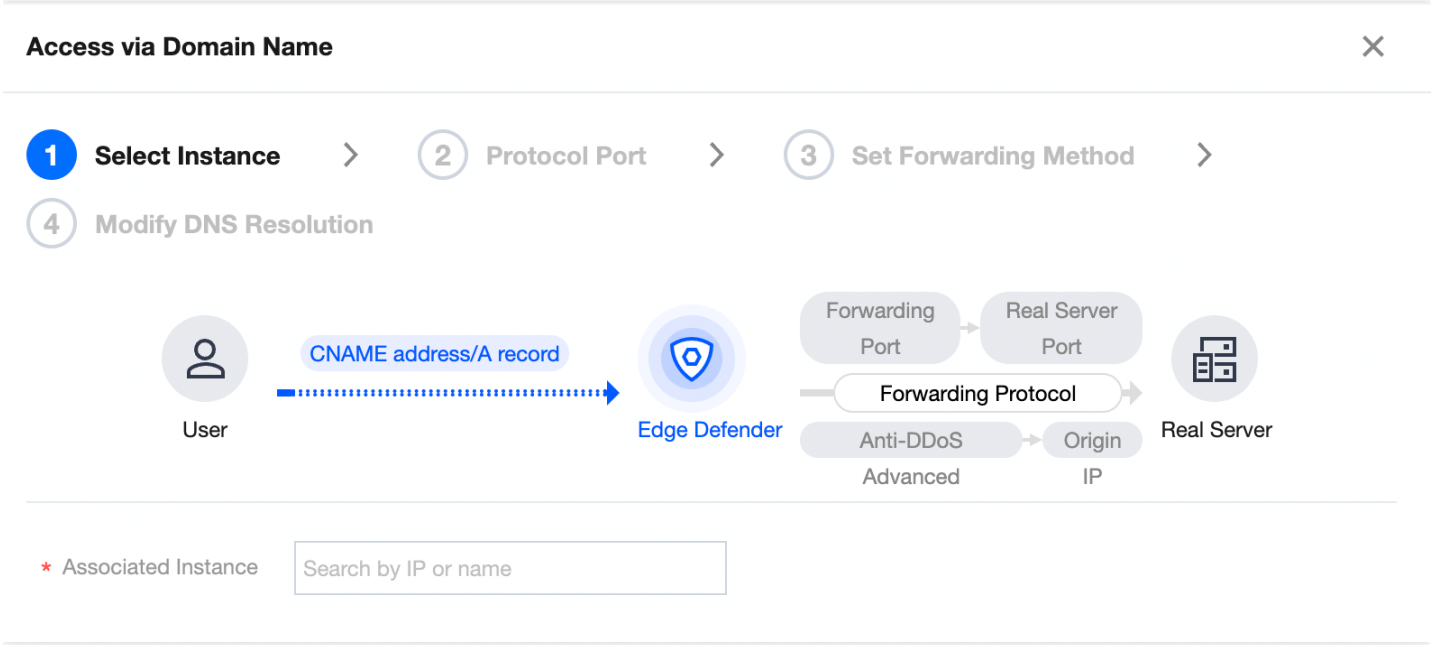
Accessing a Rule

1. Log in to the Anti-DDoS Advanced Console, select **Anti-DDoS Advanced (New)** > **Application Accessing** on the left sidebar, and then open the **Access via domain names** tab.
2. Click **Start Access**.

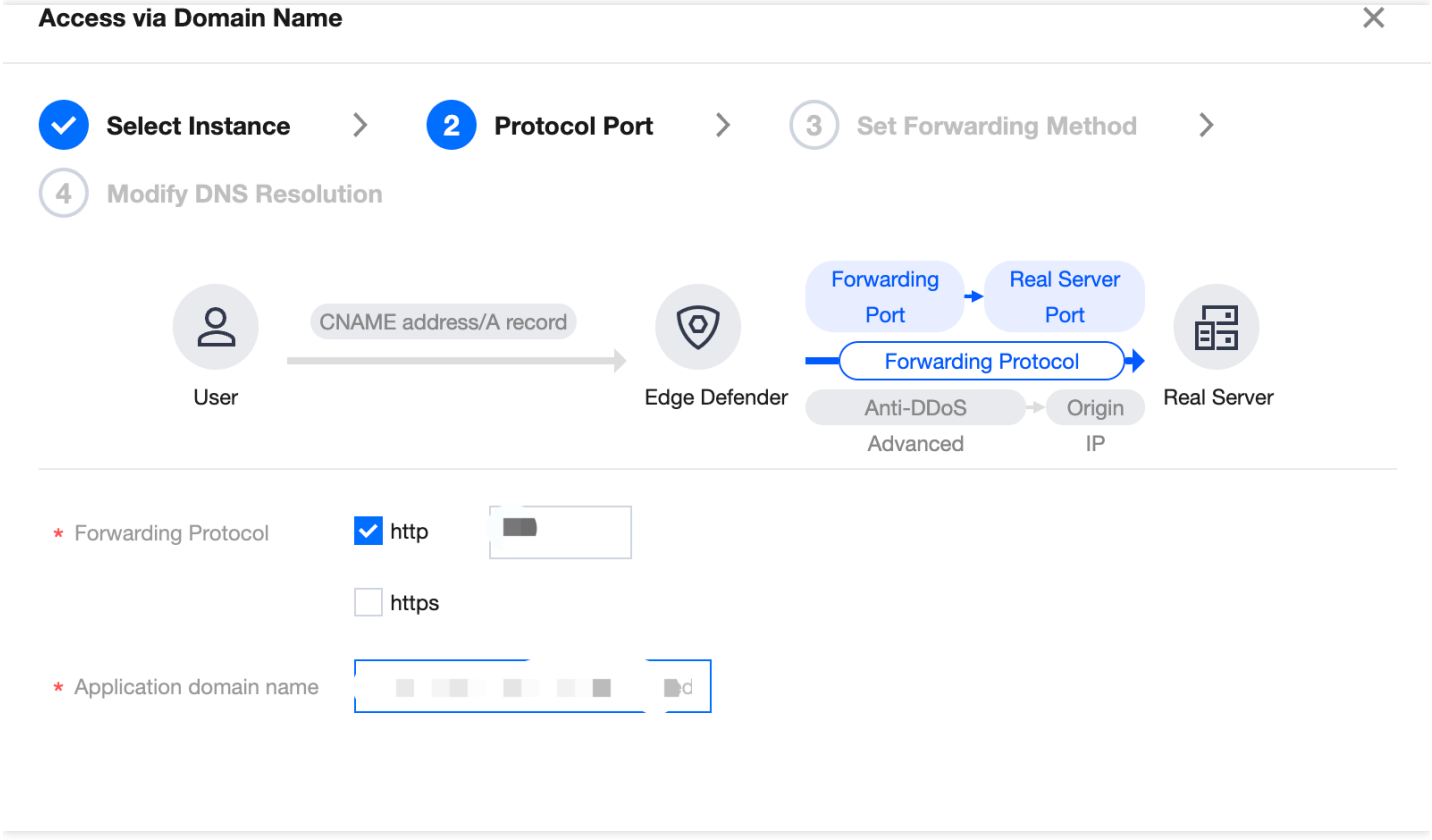


3. On the **Access via Domain Name** page, select an associated instance ID and click **Next: Set Port Parameter**.

Note：
You can select multiple instances.

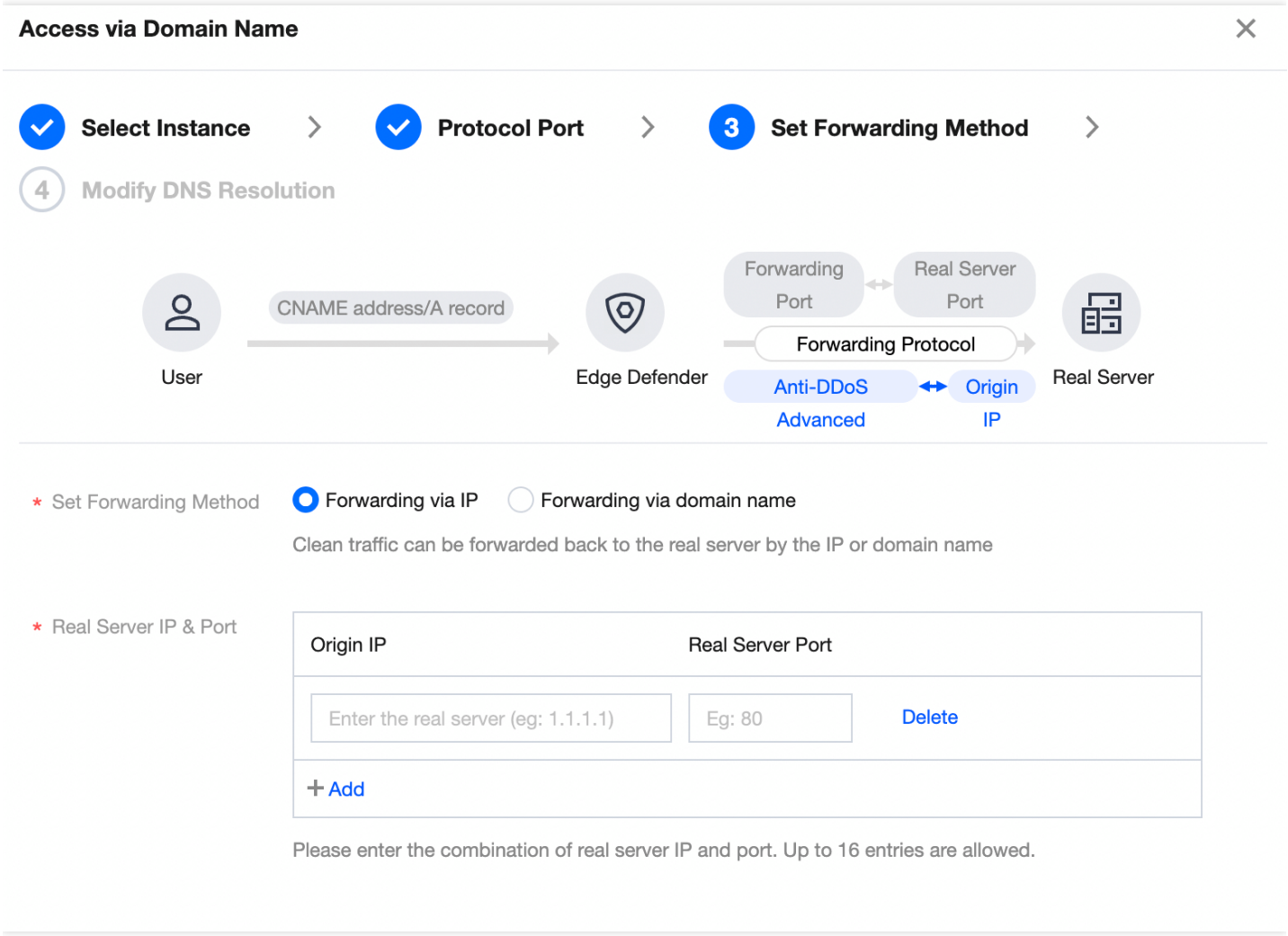


3. Select a forwarding protocol, specify a domain name, and then click **Next: Set Forwarding Method**.



4. Select a forwarding method, specify a "real server IP+port"/real sever domain name, and add an alternate real

server and set the weight if you have one. Then click **Next: Modify DNS Resolution**.



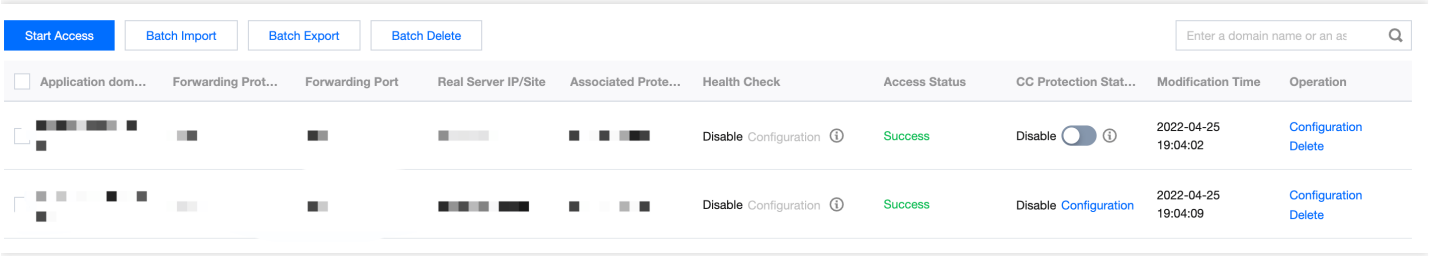
Note：

An alternate real server is used when the real server's forwarding fails.

5. Click **Complete**. Rules that are added will display in the domain name list. You can check whether they access via the domain names successfully.

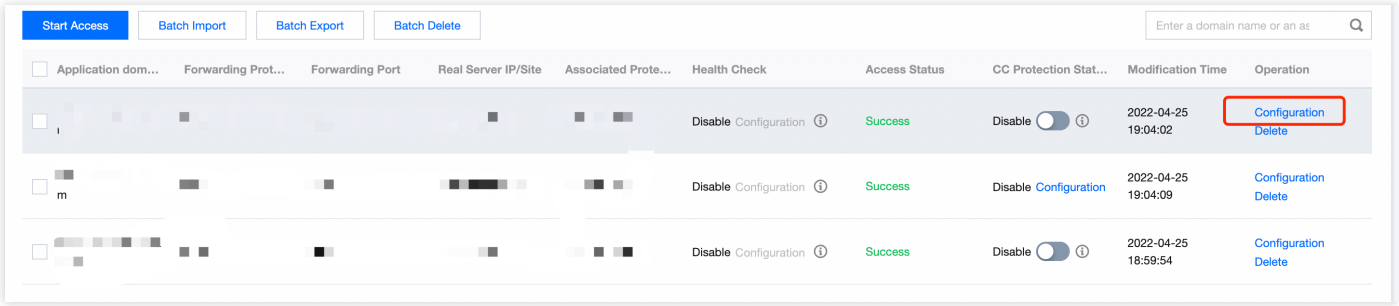
Note：

- When the access fails due to certification configuration errors, you will get a prompt "Failed to obtain the certificate. Please go to SSL Certificate Management to view details".
- To avoid seconds of interruptions, update the certificate for connected domain names during off-peak periods.

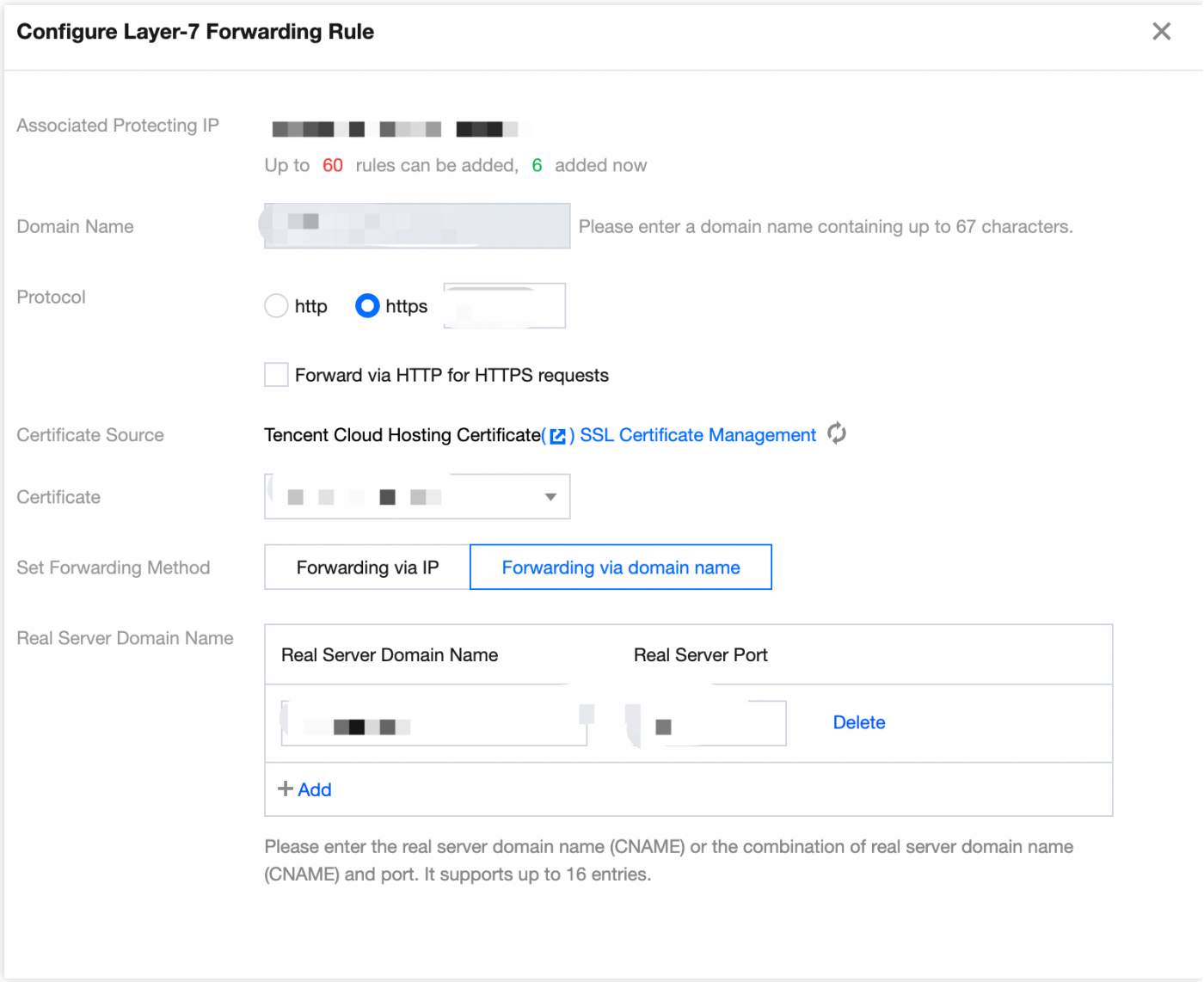


Editing a Rule

1. On the Access via domain names page, select a rule you want to edit and click **Configuration**.



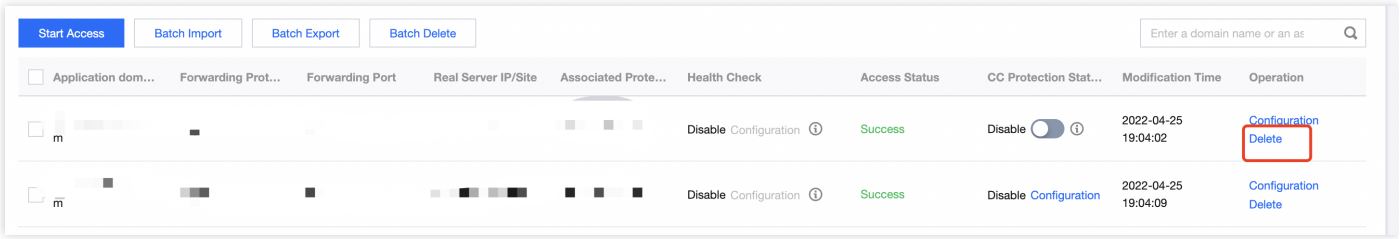
2. On the **Configure Layer-7 Forwarding Rule** page, modify parameters and click **OK** to save changes.



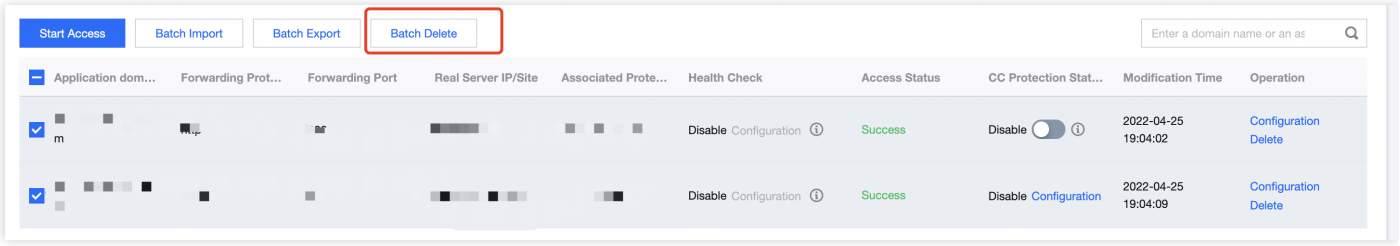
Deleting Rules

1. On the **Access via domain names**, you can delete one or more rules.

- To delete a rule, select a rule you want to delete. Click **Delete**.



- To delete multiple rules, select more than one rules you want to delete. Click **Batch Delete**.

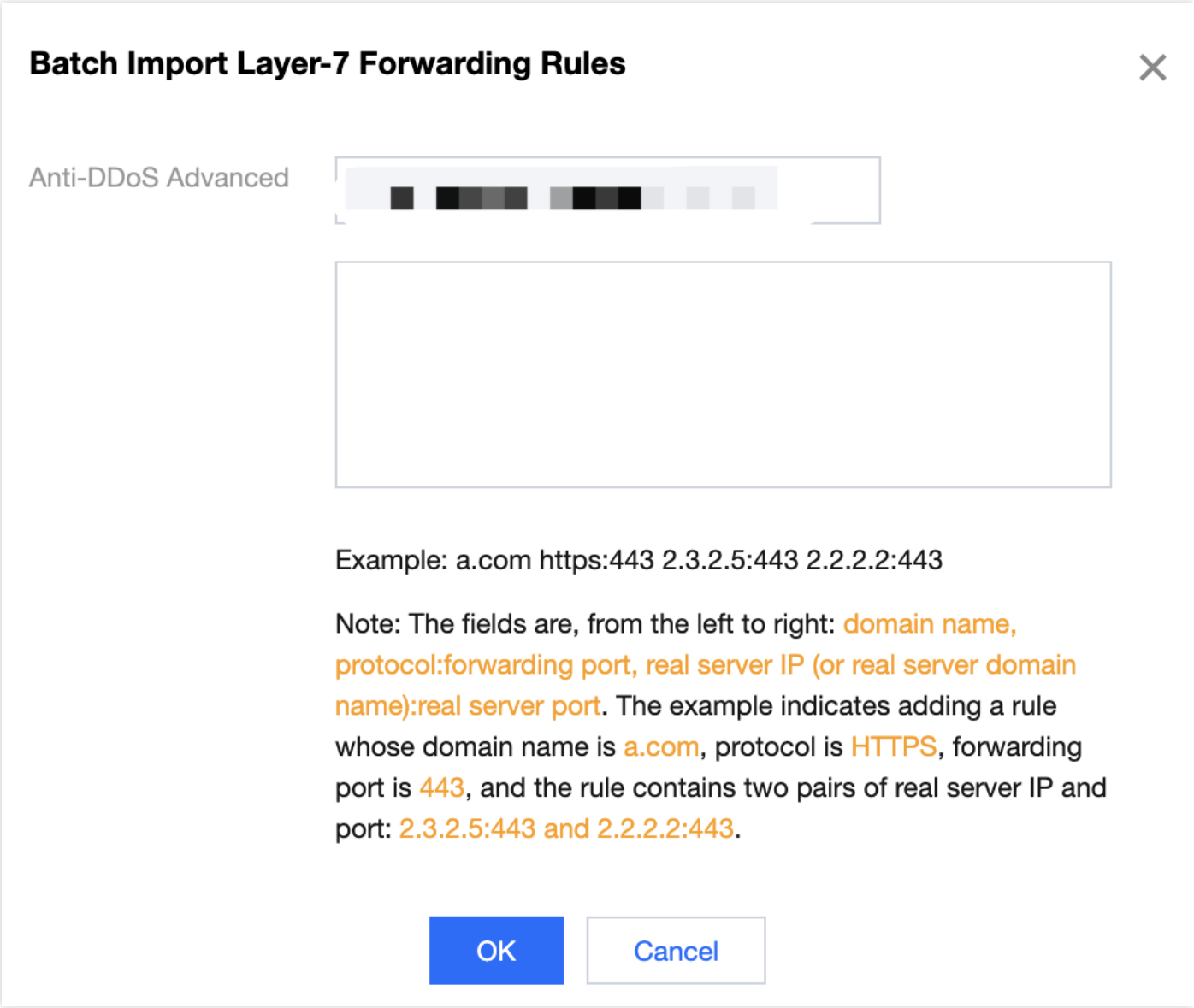


2. In the pop-up window, click **Delete**.

Importing a Rule

1. To import multiple rules, you can click **Batch Import**.

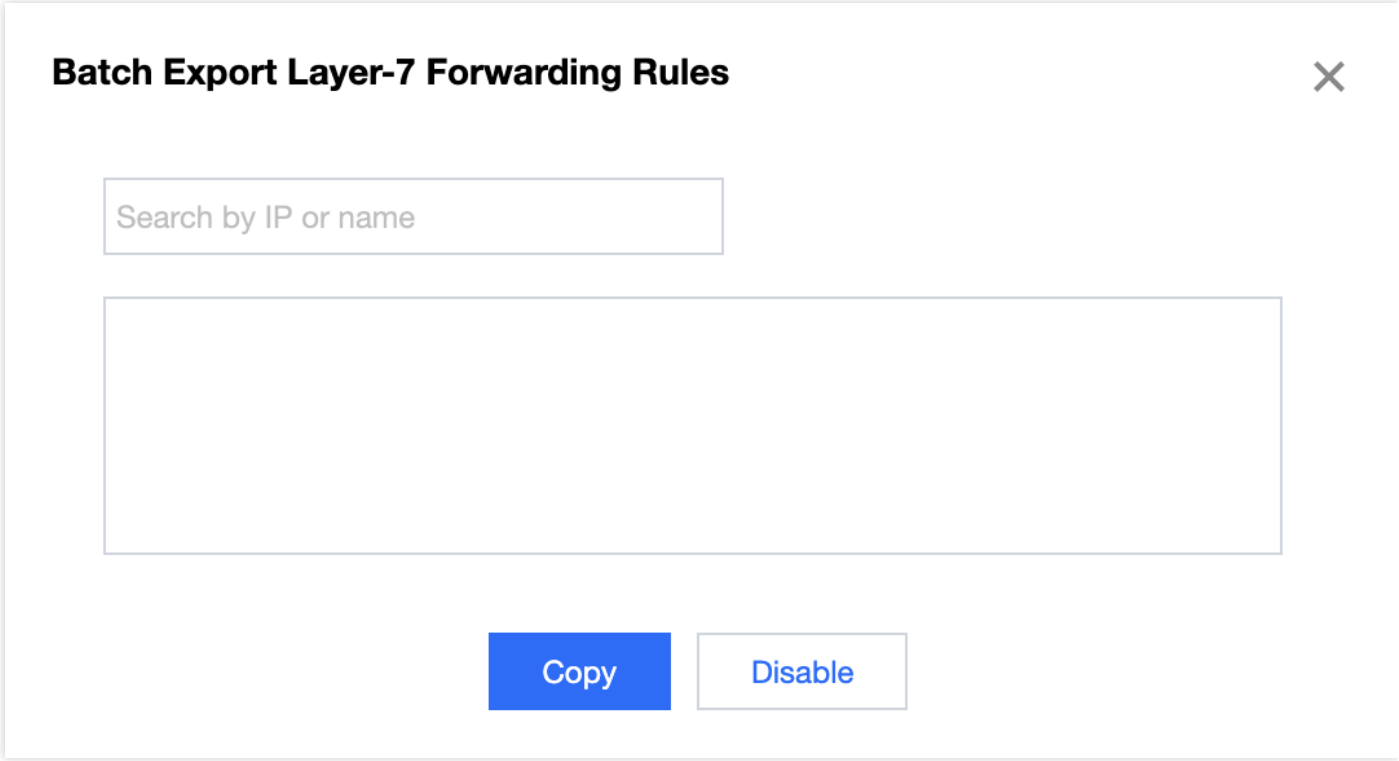
2. In the **Configure Layer-7 Forwarding Rule** window, enter the rules, and click **OK.



Exporting a Rule

1. To import multiple rules, you can click **Batch Export**.

2. In the **Batch Export Layer-7 Forwarding Rules** window, select the rules you want to export, and click **Copy**.



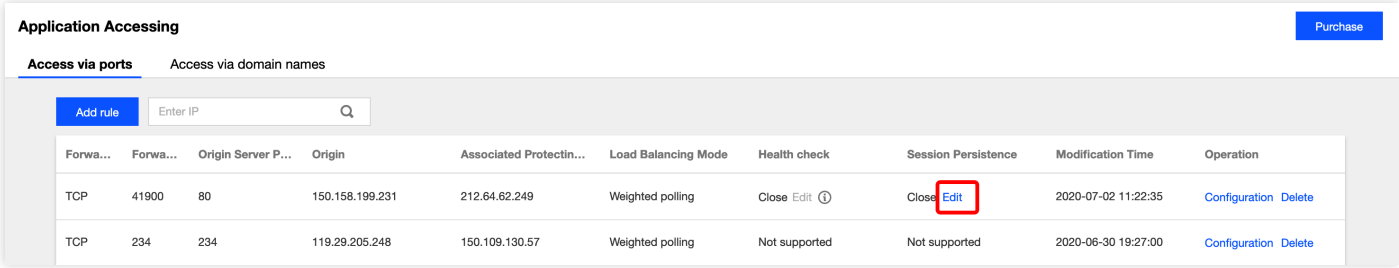
Configuring Session Persistence

Last updated：2022-04-28 14:48:00

The non-website business protection service of Anti-DDoS Advanced provides IP-based session persistence to support forwarding requests from the same IP address to the same real server for processing.
Layer-4 forwarding supports simple session persistence. The session persistence duration can be set to any integer between 30 and 3,600 seconds. If the time threshold is exceeded and the session has no new request, the connection will be automatically closed.

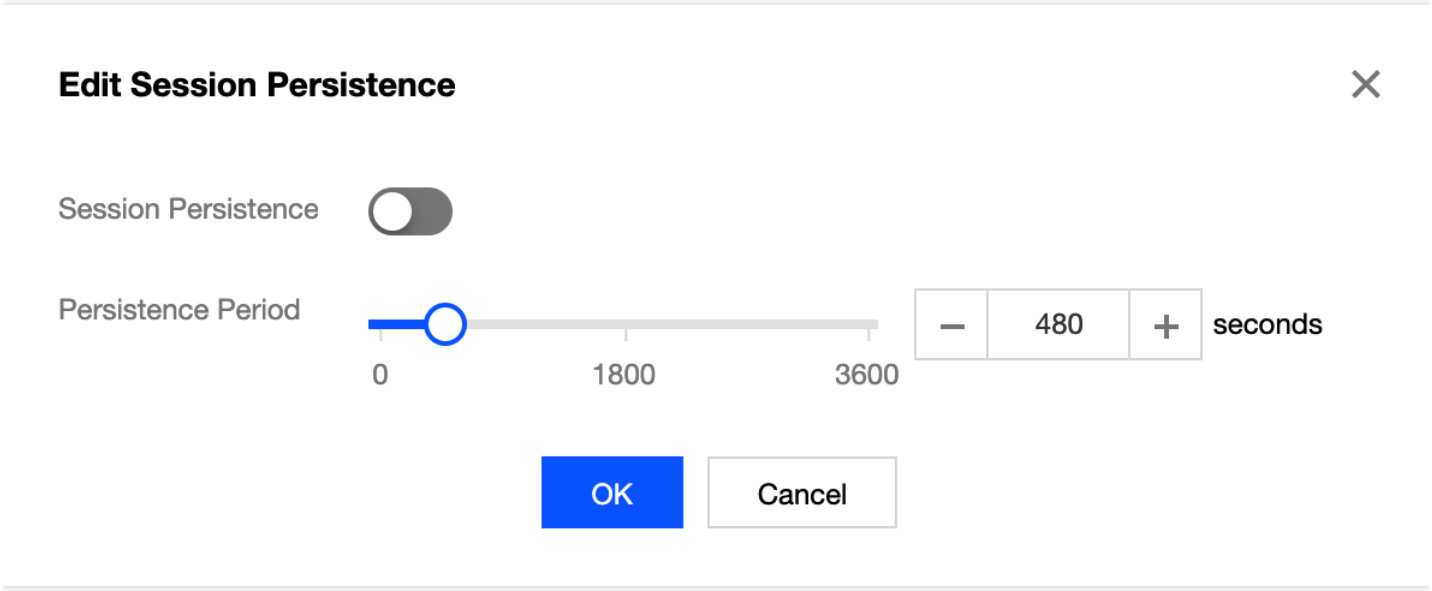
Directions

1. Log in to the new Anti-DDoS Advanced Console and click **Business Connection** > **Port Connection** .
2. On the "Port Connection" tab, select the target Anti-DDoS Advanced instance and the corresponding rule and click **Edit** in the "Session Persistence" column.



3. On the session persistence editing page, set the persistence duration and click **OK**.

> Note：
> Session persistence is disabled by default. When setting the persistence duration, you are recommended to use the default value.



Instance Management
Viewing Instance Information

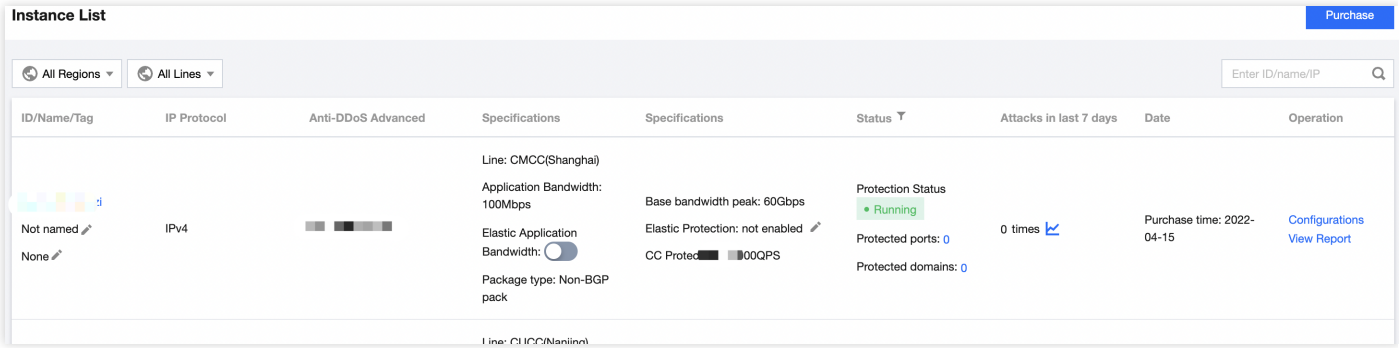
Last updated：2022-08-16 15:28:12

You can view the basic information (such as the base protection bandwidth and running status) and elastic protection configuration of your purchased Anti-DDoS Advanced instances in the console.

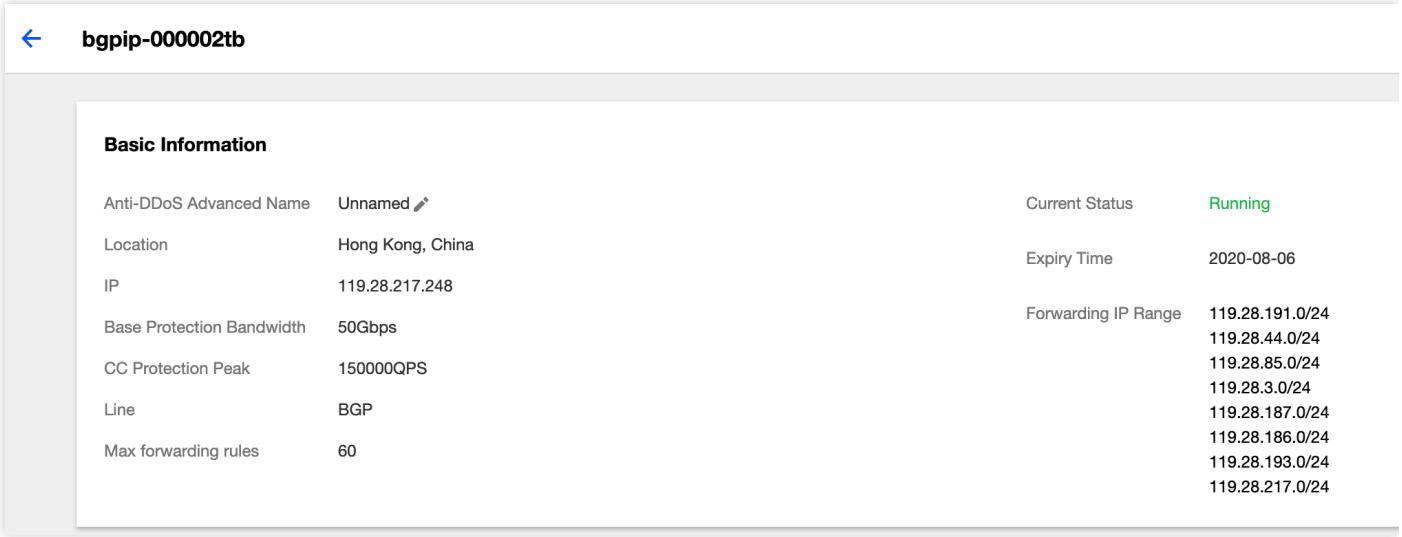
Directions

The following takes the Anti-DDoS Advanced instance "bgpip-000002jf" as an example.

1. Log in to the Anti-DDoS Advanced Console. Select **Anti-DDoS Advanced (New)** > **Instance List** on the left sidebar. Select a target instance and click the ID to view the instance details. If you have many instances, you can use the search box in the top right corner to filter results.



2. On the pop-up page, you can view the following information:



- **Anti-DDoS Advanced Name**: Name of the Anti-DDos Advanced instance, which allows you to identify and manage instances. You can create a instance name containing 1–20 characters of any type as desired.
- **Destination IP**: The IP address of Anti-DDoS Advanced instance. The IP address may change.

  Note：
  To avoid DNS resolution failure, you are recommended to change the DNS resolution address to the assigned CNAME.

- **Region**: Select a region when purchasing an Anti-DDoS Advanced instance.
- **CNAME**: CNAME of the Anti-DDoS Advanced instance. The CNAME will be resolved to an instance IP that can forward cleansed traffic to the origin server.

  Note：
  To avoid DNS resolution failure, you are recommended to change the DNS resolution address to the assigned CNAME.

- **Base protection bandwidth**: Base protection bandwidth of the Anti-DDoS Advanced instance, that is, the **base protection bandwidth** you select when you purchase the instance. If the elastic protection is disabled, the base protection bandwidth is the maximum bandwidth of the instance.
- **Current Status**: Current status of the Anti-DDoS Advanced instance, such as **Running**, **Cleansing**, and **Blocking**.
- **Expiration Time**: It is calculated based on the purchase duration selected when the instance is purchased and the time when the order is paid, which is accurate to second. Tencent Cloud will send expiration and renewal reminders to the account creator and all collaborators through Message Center, SMS, and email within 7 days before the instance expires.
  - **Tag**: Tag of the Anti-DDoS Advanced instance, which can be edited and deleted.
  - **Intermediate IP Range**: IP that forwards cleansed traffic back to the origin server.

Setting Instance Alias and Tag

Last updated：2020-07-07 17:19:16

When multiple Anti-DDoS Advanced instances are used, you can set "resource names" to quickly identify and manage them.

Prerequisites

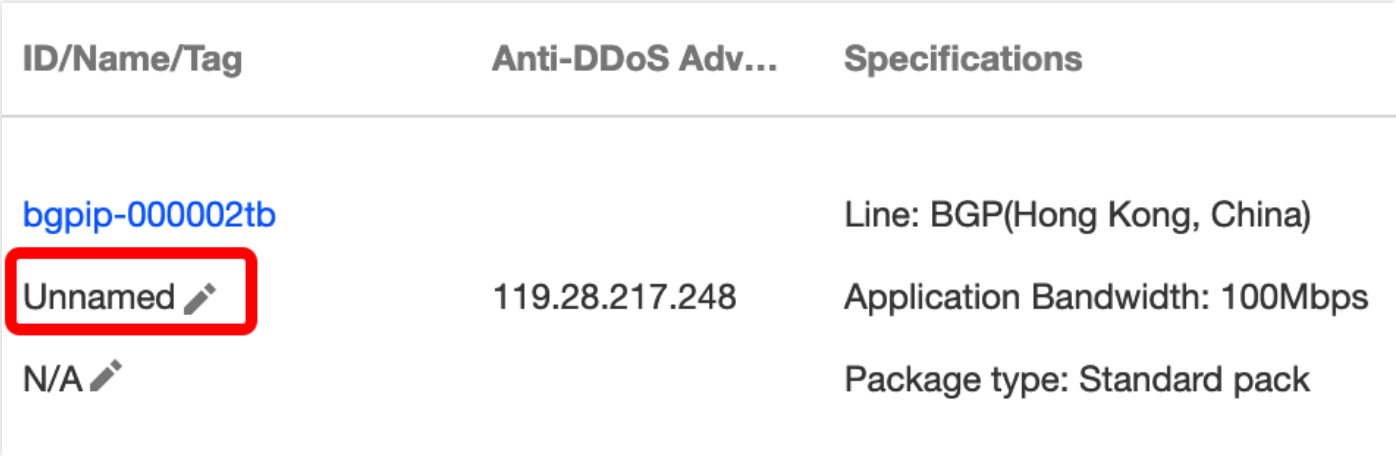
You need to purchase an Anti-DDoS Advanced instance first.

Directions

Method 1

1. Log in to the new Anti-DDoS Advanced Console and click **Instance List** on the left sidebar.
2. In the instance list, click the second row in the "ID/Name/Tag" column of the target instance and enter a name.

> The name can contain 1–20 characters of any type.

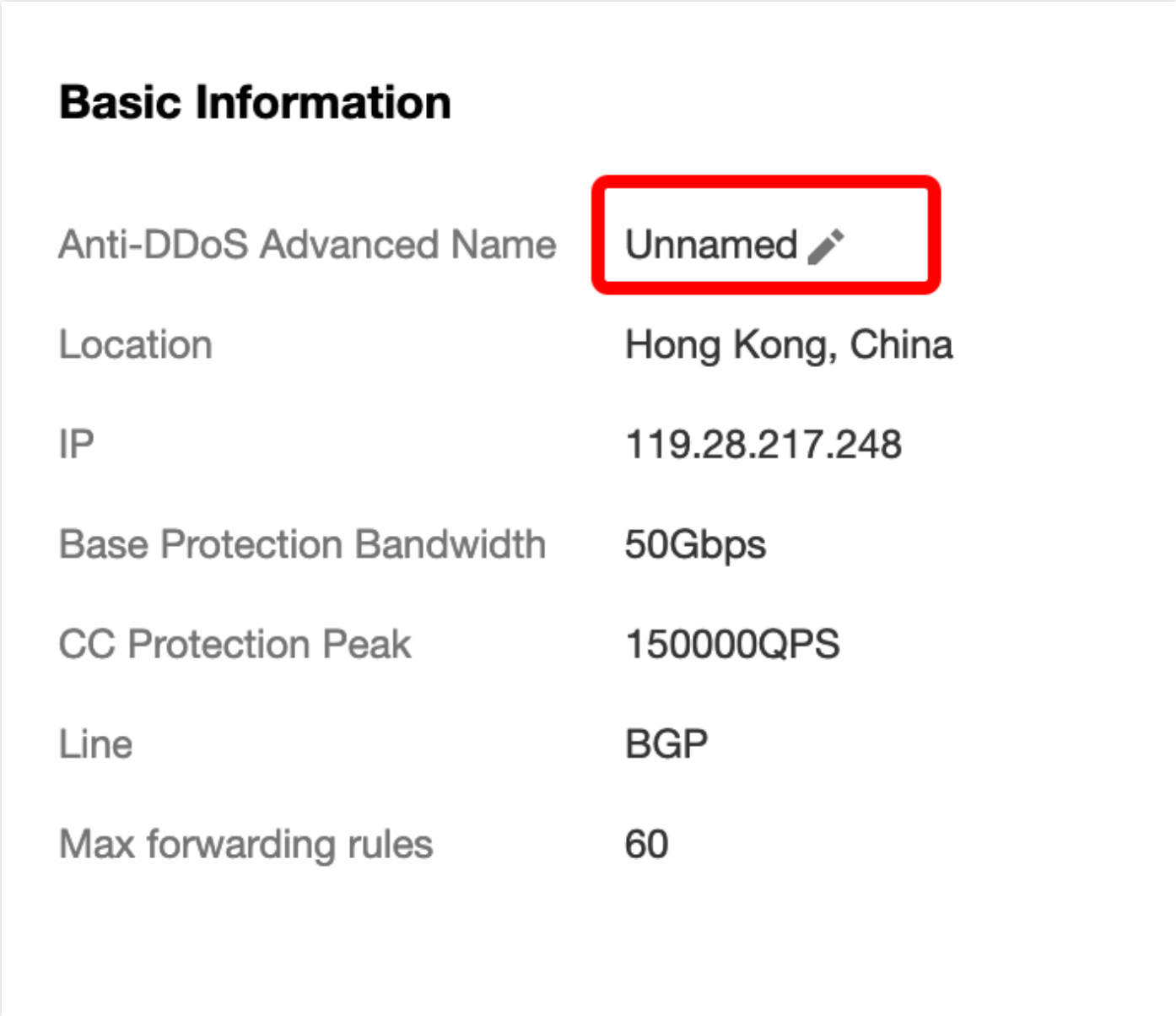


Method 2

1. Log in to the new Anti-DDoS Advanced Console and click **Instance List** on the left sidebar.
2. In the instance list, click the ID in the "ID/Name/Tag" column of the target instance to enter the instance basic information page.

3. On the basic information page of the instance, click the "Modify" pencil icon on the right of the instance name and enter a name.

> The name can contain 1–20 characters of any type.



Configuring Intelligent Scheduling

Last updated：2022-08-04 11:20:56

Use Cases

Each account can have multiple Anti-DDoS instances, and each instance has at least one protective line; therefore, there can be multiple protective lines under one account. Once your business is added to an Anti-DDoS instance, a protective line will be configured for it. If multiple protective lines have been configured, you need to choose the optimal business traffic scheduling method, i.e., how to schedule business traffic to the optimal line for protection while ensuring high business access speed and availability.
Anti-DDoS features priority-based CNAME intelligent scheduling, where you can select an Anti-DDoS instance and set the priority of its protective line as needed.

> Note：
> DNS configuration is supported for Anti-DDoS Pro instances and Anti-DDoS Advanced instances (including instances for BGP, China Telecom, China Unicom, and China Mobile).

Priority-based Scheduling

This refers to using the protective line of the highest priority to respond to all DNS requests, i.e., all access traffic will be scheduled to the protective line of the currently highest priority. You can adjust the priority value of a protective line, which is 100 by default. The smaller the value, the higher the priority. The specific scheduling rules are as follows:

- If the Anti-DDoS instance configured for your business contains multiple protective lines from different ISPs and of the same priority, response will be made based on the ISP of the specific DNS request. If one of the lines is blocked, access traffic will be scheduled in the order of BGP > China Telecom > China Unicom > China Mobile > ISPs outside Mainland China (including those in Hong Kong (China) and Taiwan (China)).
- If all the lines of the same priority are blocked, access traffic will be automatically scheduled to the currently available protective line of the second-highest priority.

> Note：
> If no protective lines of the second-highest priority are available, automatic scheduling cannot be completed, and business access will be interrupted.

- If the Anti-DDoS instance configured for your business contains multiple protective lines from the same ISP and of the same priority, access traffic will be scheduled by way of load balancing, i.e., evenly distributed to such lines.

Example

Suppose you have the following Anti-DDoS instances: BGP IPs `1.1.1.1` and `1.1.1.2`, China Telecom IP `2.2.2.2`, and China Unicom IP `3.3.3.3`, of which the priority of `1.1.1.2` is 2 and that of the rest is 1. Normally, all traffic will be scheduled to the protective lines with the current priority of 1. Specifically, traffic from China Unicom will be scheduled to `3.3.3.3`, that from China Telecom to `2.2.2.2`, and that from other ISPs to `1.1.1.1`. If `1.1.1.1` is blocked, access traffic under this IP will be automatically scheduled to `2.2.2.2`. If both `1.1.1.1` and `3.3.3.3` are blocked, traffic supposed to be scheduled to them will be distributed to `2.2.2.2`, and if `2.2.2.2` is blocked too, traffic will be scheduled to `1.1.1.2`.

Prerequisites

- Before enabling intelligent scheduling, please connect your business to be protected to your Anti-DDoS instance.

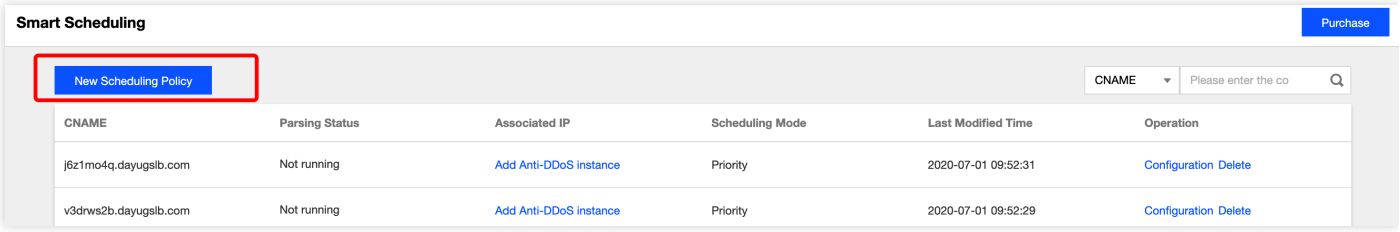
> Note：
>
> - If you need to add the IP of your protected Tencent Cloud service to a purchased Anti-DDoS Pro instance, please see Getting Started with Anti-DDoS Pro.
> - If you need to connect your layer-4 or layer-7 application to a purchased Anti-DDoS Advanced instance, please see Anti-DDoS Advanced documents Port Connection or Domain Name Connection.

- To modify the DNS resolution, you need to purchase the domain name resolution product.

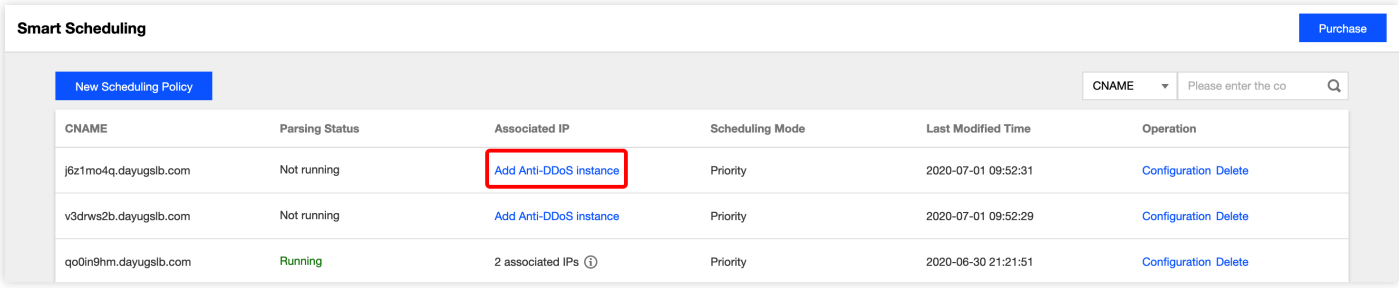
Setting Line Priority

Please follow the steps below to set priorities for your Anti-DDoS instance based on your scheduling scheme:

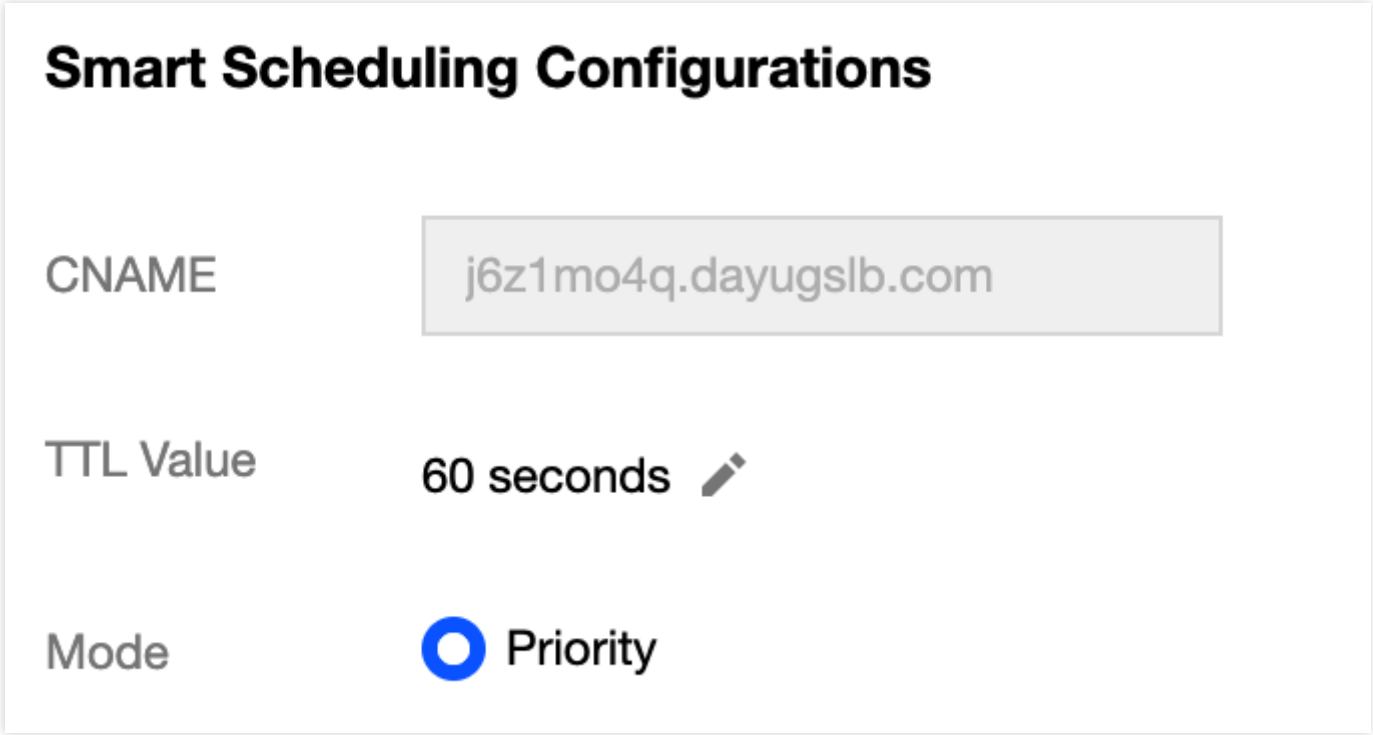
1. Log in to the new Anti-DDoS Advanced Console and click **Intelligent Scheduling** on the left sidebar to enter the list page. Click **Add Scheduling**, and the system will automatically generate a CNAME record.



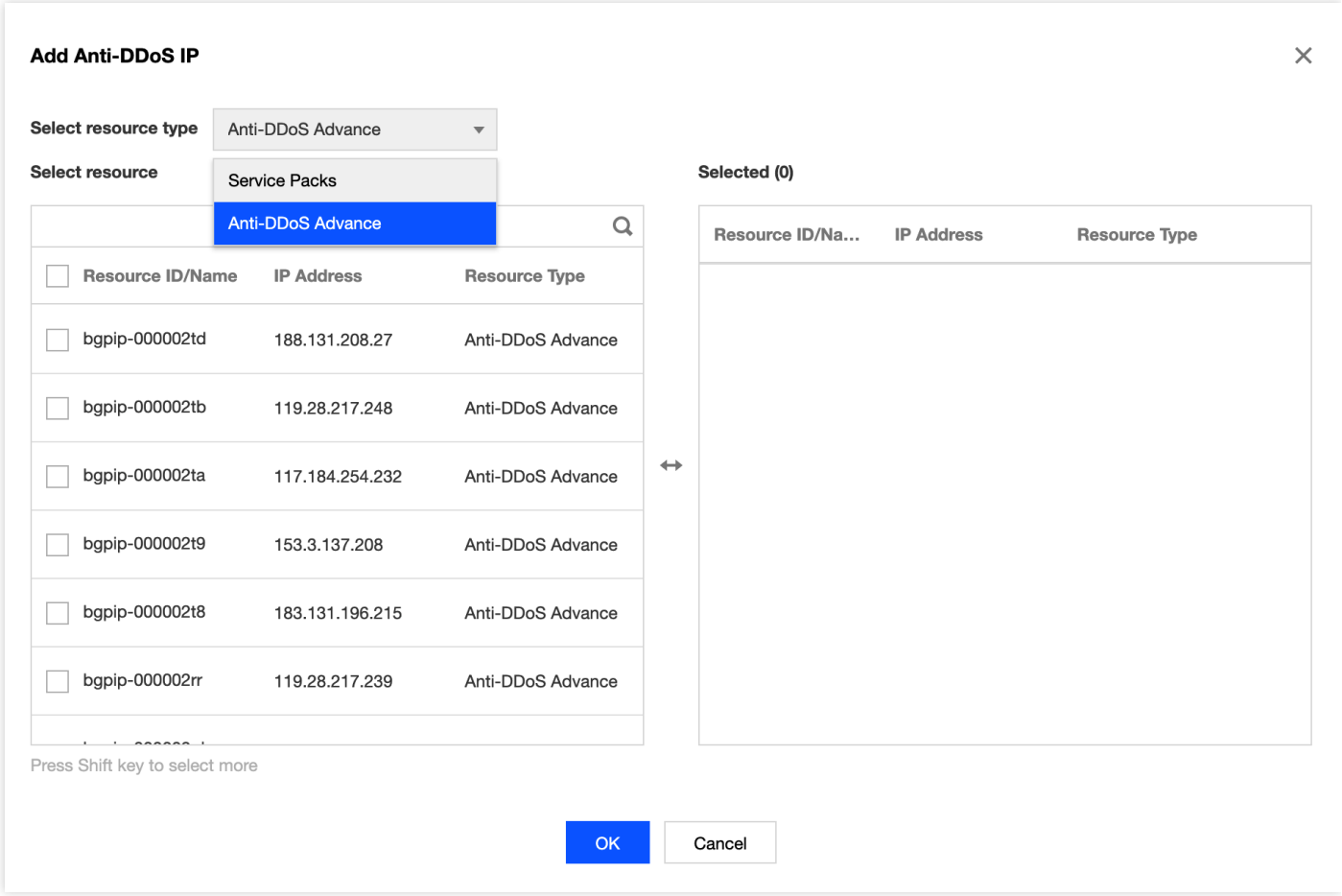
2. Locate the row of the CNAME record and click **Add Anti-DDoS Instance** to enter the intelligent scheduling editing page.



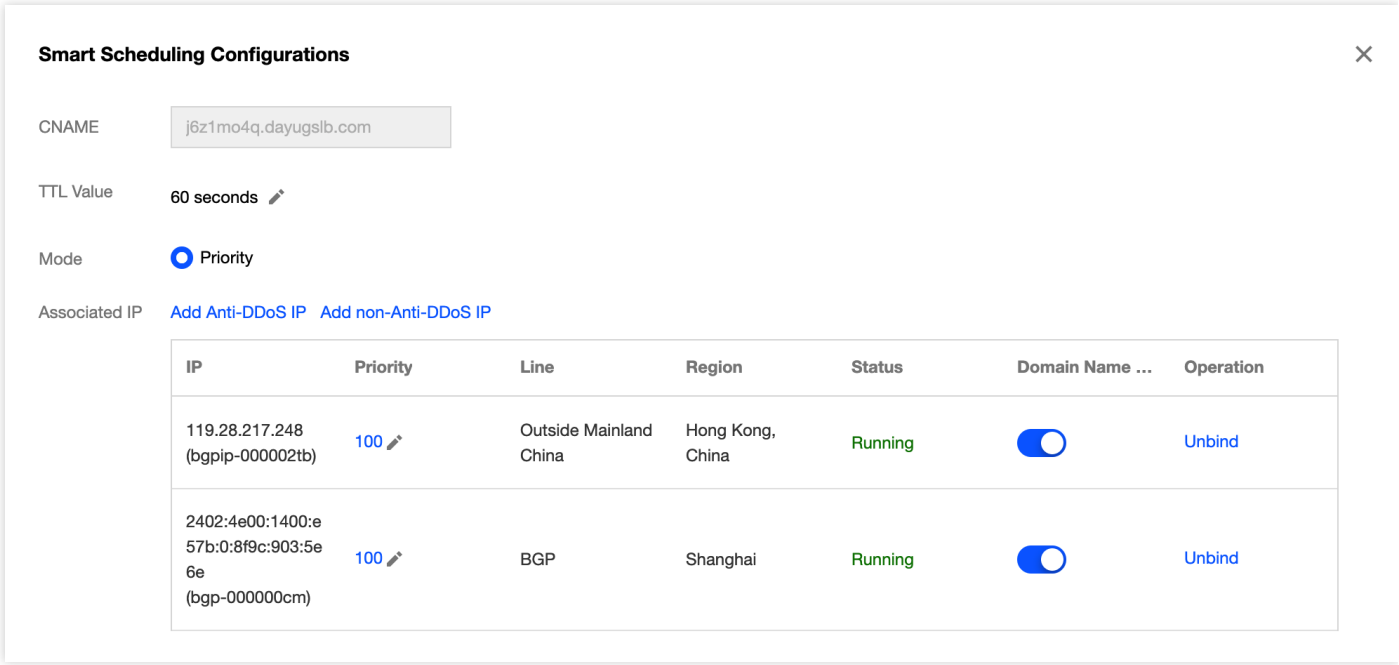
3. On the intelligent scheduling editing page, the TTL value is 60s by default, which can range from 1s to 3,600s, and the default scheduling method is priority-based.



4. Click **Add Anti-DDoS Resource IP**, select the target Anti-DDoS Advanced instance and IP, and click **OK**.



5. After the instance is selected, domain name resolution will be enabled for its protective line by default. At this point, you can set the line priority.



Example

Suppose you want to implement the following scheme: the business traffic will be scheduled to a BGP protective line first; if it is blocked due to attacks, the traffic will be automatically scheduled to a China Telecom protective line; if it is also blocked, the traffic will be scheduled to a China Unicom protective line; and after the BGP protective line is unblocked, the traffic will be scheduled to it automatically.
To implement this scheduling scheme, set the priority of the BGP line in the Anti-DDoS instance to 1 and that of the China Telecom line to 2, and keep the priority of the China Unicom line unchanged.

IP	Priority	Line	Region	Status	Domain Name ...	Operation
183.131.196.215 (bgpip-000002t8)	100	CTCC	Hangzhou	Running		Unbind
153.3.137.208 (bgpip-000002t9)	100	CUCC	Nanjing	Running		Unbind
2402:4e00:1400:e57b:0:8f9c:903:5e6e (bgp-000000cm)	100	BGP	Shanghai	Running		Unbind

If you do not want the China Unicom protective line to be in the traffic scheduling scheme, click  to disable domain name resolution for it, and you can enable domain name resolution again and set its priority when necessary.

If you want to delete it from the current scheduling scheme, you can locate the row of its corresponding instance and click **Unbind**.

Modifying DNS Resolution

Before using a CNAME record for intelligent scheduling, you are recommended to change the CNAME record of your business domain name DNS to the CNAME record automatically generated by the intelligent scheduling system of Tencent Cloud Anti-DDoS, to which all access traffic to your business website will be directed.

Setting Security Event Notification

Last updated：2020-07-07 17:19:18

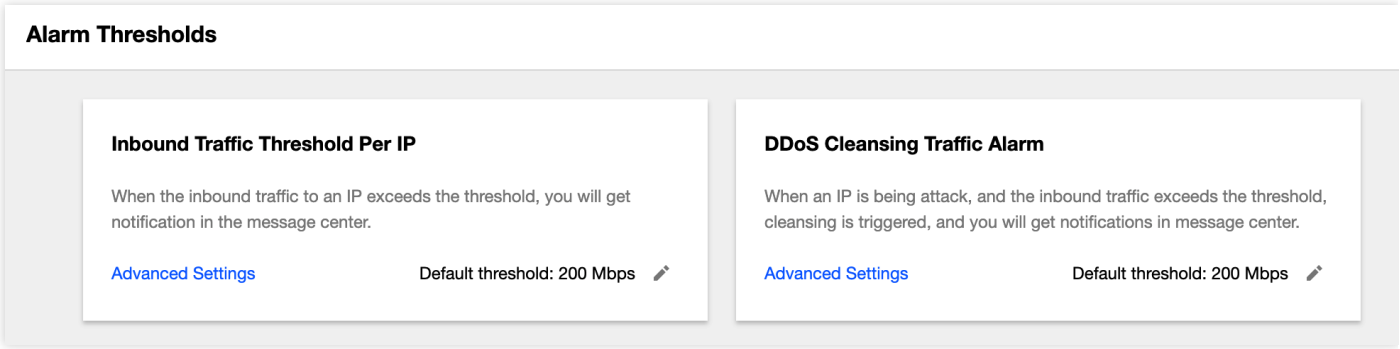
Alarm messages for Anti-DDoS Advanced will be sent to you through Message Center, SMS, or email in the following conditions (the receipt methods configured on the Message Center Subscription page shall prevail):

- An attack starts.
- An attack ended 15 minutes ago.
- An IP is blocked.
- An IP is unblocked.

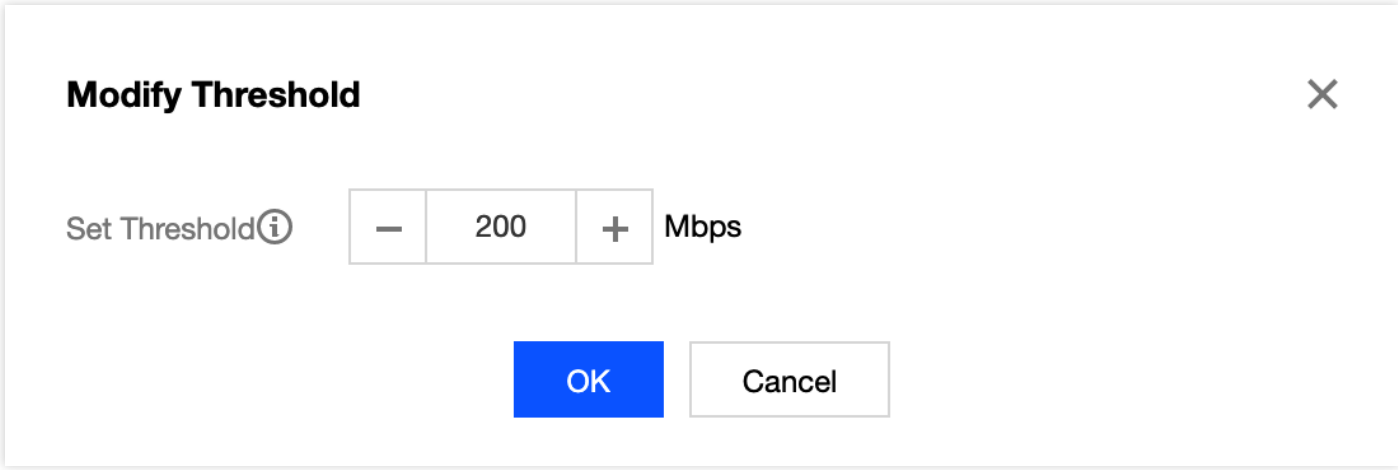
You can modify the recipients and how they receive the alarm messages as needed.

Setting Alarm Threshold

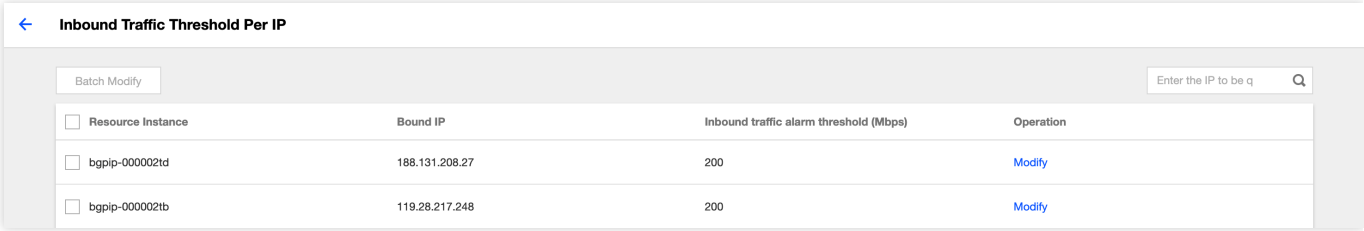
1. Log in to the new Anti-DDoS Advanced Console and select **Alarm Notification** on the left sidebar.
2. You can set the "inbound traffic alarm threshold for single IP" and "DDoS cleansing threshold" in the feature blocks on the right.



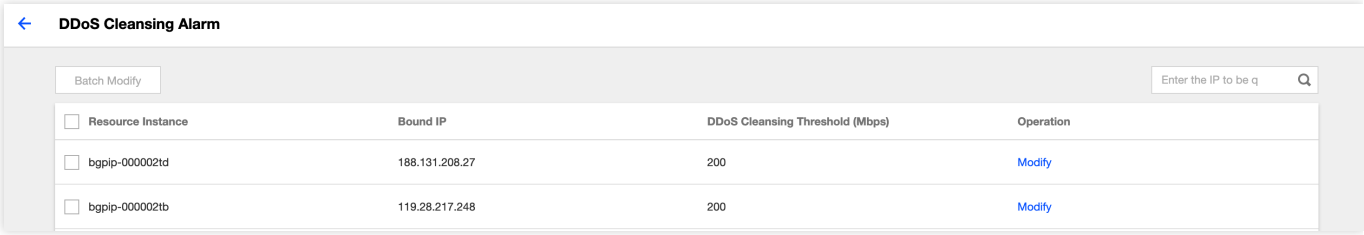
3. Click the pencil icon on the right of the default threshold for one single IP to modify the default threshold. After the modification is completed, click **OK**.



4. Click **Advanced Settings** in a block to enter the IP alarm settings list, where you can set different alarm thresholds for different IPs.
   - Inbound traffic alarm for single IP



   - DDoS cleansing threshold

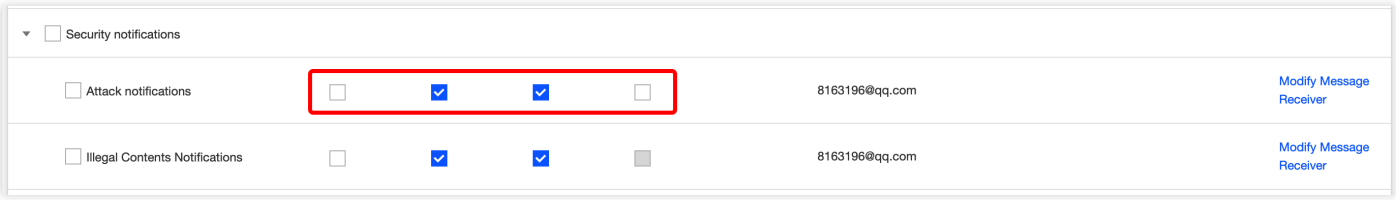


Setting Notification Method

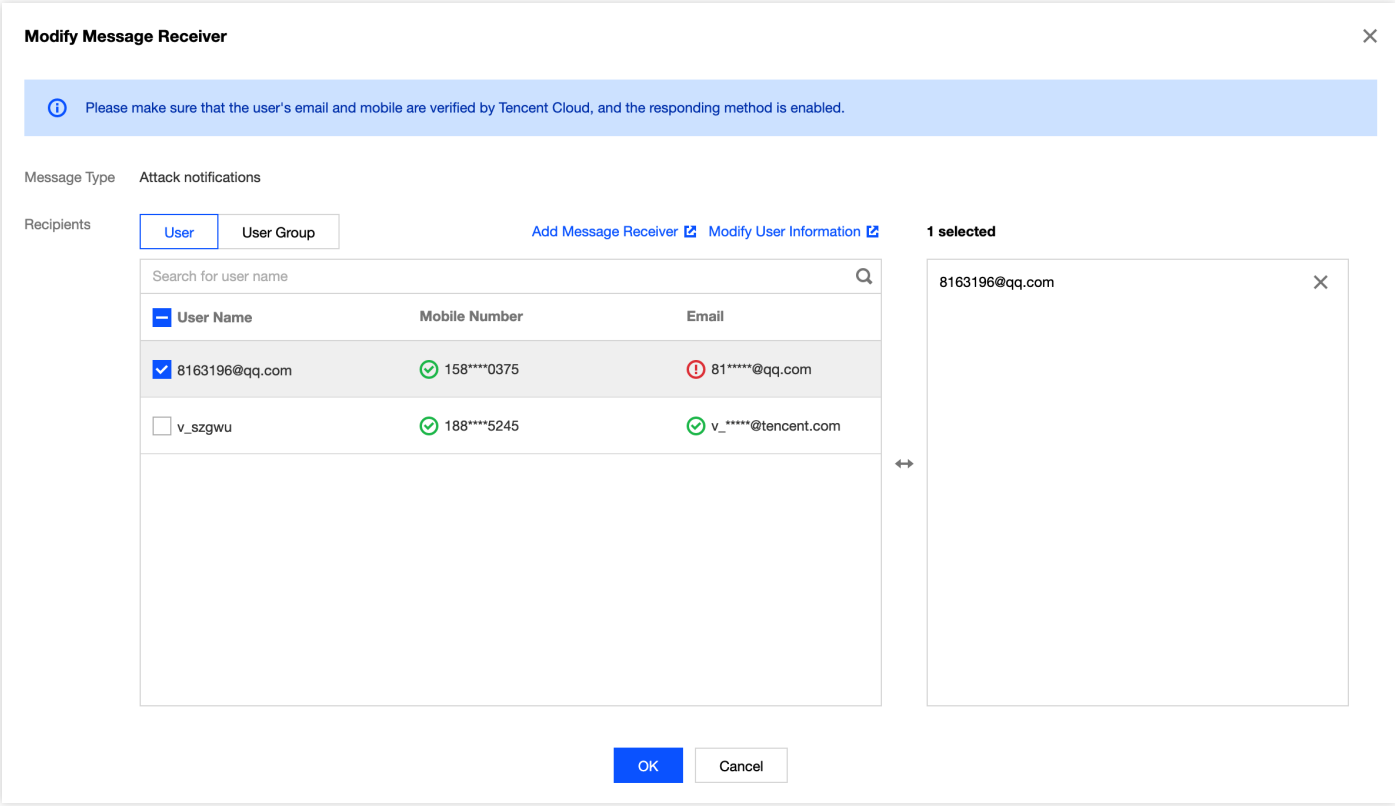
1. Log in to your Tencent Cloud account and go to the Message Center.

> Alternatively, you can log in to the console, click in the top-right corner, and then click **View More** in the pop-up window to enter the Message Center.

2. Click **Message Subscription** on the left sidebar to enter the message list.
3. In the message list, select the receipt methods on the row of **Security Event Notification** and click **Modify Message Recipient** to enter the message recipient modifying page.



4. On the message recipient modifying page, set the message recipients. After completing the settings, click **OK**.



Viewing Operation Log

Last updated：2020-07-07 17:19:18

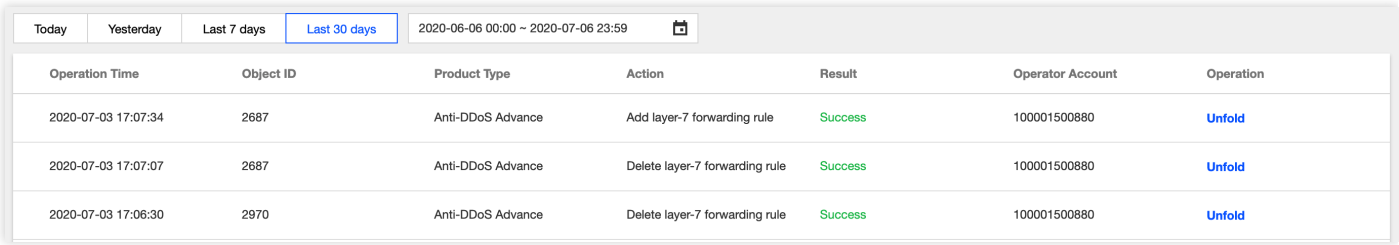
Operation Scenarios

Anti-DDoS Advanced allows you to view logs of important operations in the last 90 days in the console. The following types of logs are available:

- Logs of forwarding rule change
- Logs of protection policy change
- Logs of cleansing threshold adjustment
- Logs of protection level change
- Logs of instance name change

Directions

1. Log in to the new Anti-DDoS Advanced Console and click **Operation Log** on the left sidebar.
2. On the operation log page, you can query operation logs by time period. You can click **Show More** in the "Operation" column on the right to view log details.



Blocking Operations
Connecting a Blocked Server

Last updated：2023-04-28 16:51:55

This document describes how to connect a blocked server.

Directions

1. Log in to the CVM Console and click **Instances** on the left sidebar.
2. Click the drop-down list in the top left corner and modify the region.
3. Click the search box to use filters such as "Instance Name", "Instance ID" and "Instance Status" to locate the blocked server.
4. Click **Log In** for the blocked server to display the **Log in to Linux Instance** pop-up window.
5. In the pop-up window, select **Login over VNC** and click **Log In Now** to connect the server via browser VNC.

Unblocking an IP

Last updated：2022-11-23 10:55:46

Unblocking Procedure

Auto unblocking

With auto unblocking, you only need to wait until blocked IPs are unblocked automatically. You can check the predicted unblocking time as follows:

1. Log in to the Anti-DDoS console. Select **Self-Service Unblocking** > **Unblock Blocked IP** on the left sidebar to get to unblocking operation.
2. Check the predicted unblocking time of the IP in **Estimated Unblocking Time** on the unblocking page.

Chances for self-service unblocking

Only three chances of self-service unblocking are provided for Anti-DDoS Advanced every day. The system resets the chance counter daily at midnight. Unused chances cannot be accumulated for the next day.

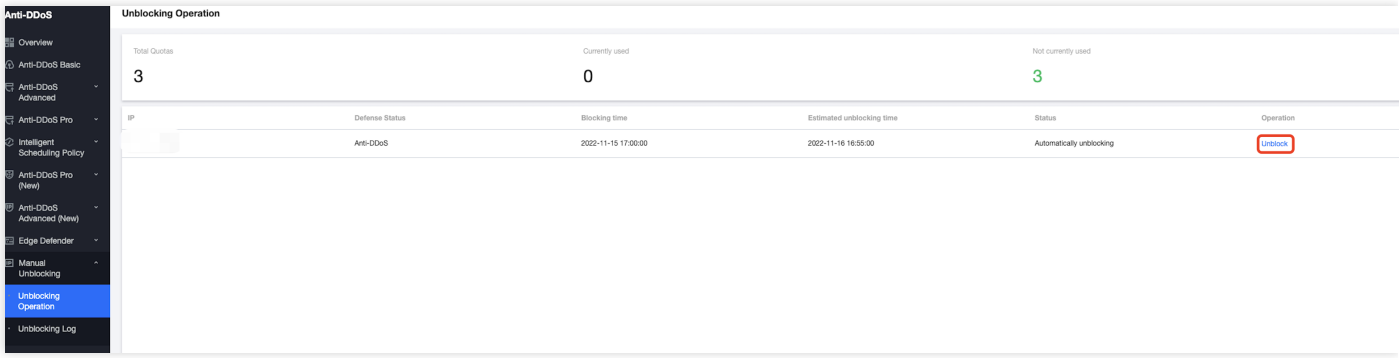
Note：

- The unblocking may fail for risk management reasons. A failed attempt does not count as a chance. Please wait for a while and then try again.
- Before unblocking the IP, please check the predicted unblocking time which may be affected by some factors and will be postponed. If you accept the predicted time, you do not need to operate manually.
- If the self-recovery chances are used up for the day, you can upgrade the base protection capability or the elastic protection capability to defend against large traffic attack and avoid continuous blocking.

Manual unblocking

1. Log in to the Anti-DDoS console. Select **Self-Service Unblocking** > **Unblock Blocked IP** on the left sidebar to get to unblocking operation.

2. Find the protected IP in **Pending Auto Unblocking** and click **Unblock** in the **Operation** column on the right.



3. Click **OK** in the **Unblock Blocked IP** dialog box. If you receive a notification indicating successful unblocking, the IP has been successfully unblocked. You can refresh the page to check whether the protected IP is in running status.

Unblocking Operation Record

Log in to the Anti-DDoS console. Select **Self-Service Unblocking** > **Unblocking History** on the left sidebar. You can check all unblocking records in the specified period, including records of automatic and manual unblocking.